이학석사학위논문

디지털 증거 압수수색에 있어서 관련성 개념에 관한 연구
– 모바일 포렌식을 중심으로 –

2015년 8월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식전공
이 무 영

디지털 증거 압수수색에 있어서 관련성 개념에 관한 연구
– 모바일 포렌식을 중심으로 –

지도교수 안 정 호

이 논문을 이무영 석사학위논문으로 제출함

2015년 5월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식전공
이 무 영

이무영의 석사학위논문을 인준함
2015년 6월

위 원 장 이 중 식 (인)

부위원장 안 정 호 (인)

위 원 백 윤 홍 (인)

국문초록

디지털 증거는 저장 매체의 대량화로 필연적으로 사건과 관련이 없는 다른 파일과 혼재되어 있는 특징이 있다. 2011년 형사소송법은 디지털 증거 압수수색은 사건과 관련된 것에 한정하여 압수를 해야 한다고 개정되었다. 하지만, 현장에서 선별 압수수색한다는 것은 기술, 시간상 한계가 있기 때문에 형사소송법에서는 원본 압수를 할 수 있는 단서조항을 두었다.

디지털 증거 원본을 압수한 수사기관은 해당 증거물에 저장되어 있는 모든 데이터를 영장에 의해 확보한 것이라고 착각을 하기 쉽다. 수사기관에서는 정당한 영장에 의해 압수수색한 디지털 증거에서 추가 범죄사실에 대한 증거가 발견되더라도 추가 영장을 발부받지 않고 그대로 증거로 사용하려고 한다. 하지만, 이렇게 되면 포괄압수수색 영장이 되는 것이고 헌법에 위배되는 사항이다. 위와 관련하여 대법원의 사건과 관련 없는 휴대폰 녹음파일에 대한 위법수집증거로 증거능력 배제한 사례가 있으며, 미국 수사실무 및 법원 역시 디지털 증거에서 다른 사건과 관련된 증거가 발견된 경우 법원에 추가로 영장을 청구해야 된다고 보고 있다.

미국의 사례 및 최근 대법원의 입장을 우리나라 수사 현실에 적용하기 위해서는 압수수색 대상에 전자정보가 포함이 되어야 한다. 법 개정 전에 법원 및 수사기관이 추가 압수수색 영장 관련하여 세미나 등을 통하여 법의 미비점을 당분간 보완해야 할 것이다.

휴대폰(스마트폰)은 디지털포렌식의 금광으로 불린다. 그만큼 중요한 증거가 많이 발견되고 있으며 그와 비례하여 개인의 사생활은 침해가 되고 있다. 휴대폰 압수 및 분석 과정에서 사건과 관련된 것

에 한정하여 출력 및 사본을 하여 개인의 사생활이 침해가 되지 않도록 주의해야 한다. 다른 증거와 달리 휴대폰에는 민감한 개인정보가 저장이 되어 있기 때문에 수사팀과 별도의 필터링팀에서 선별작업이 필요하다.

마지막으로 본 논문을 기초로 수사의 효율성 및 개인의 인권보장 양 측면을 만족시키는 디지털 증거 수사가 이루어지길 바란다.

주요어 : 디지털 증거, 디지털 포렌식, 모바일, 압수수색, 관련성

학번 : 2013-24054

목 차

Ⅰ. 서론

현대 사회는 거의 모든 것을 디지털로 변화시키고 있다. 구글에서는 지금까지 출간한 모든 책에 대하여 디지털화 작업을 하고 있다. 개인의 일상생활을 들여다보면 거의 모든 것이 디지털로 된 것을 확인할 수 있다. 특히, 스마트폰의 이용 확대로 디지털은 한 개인의 모든 연대기를 저장하고 있기까지 한다. 이러한 상황에서 디지털저장매체에 저장이 되어 있는 증거를 어떻게 확보를 해야 하는지가 중요하다.

예를 들어 스마트폰에는 사건과 관련된 증거가 저장되어 있는 반면, 사건과 관련성이 전혀 없는 민감한 개인정보 및 사건과 별건의 범죄사실에 대한 증거가 있을 수 있다. 이러한 경우 사건과 관련성 있는 증거를 어떻게 선별하여 압수수색을 하는 것이 문제가 된다.

2014. 1. 16. 우리나라 대법원에서는 휴대폰 녹음파일에 대한 사건과의 관련성 여부에 대한 판결을 내렸다. 수사기관이 피의자 甲의 공직선거법 위반 범행을 영장 범죄사실로 하여 발부받은 압수·수색영장의 집행 과정에서 乙,丙사이의 대화가 녹음된 녹음파일(이하 '녹음파일'이라 한다)을 압수하여 乙,丙의 공직선거법 위반 혐의사실을 발견한 사안에서, 압수·수색영장에 기재된 '피의자'인 甲이 녹음파일에 의하여 의심되는 혐의사실과 무관한 이상, 수사기관이 별도의 압수·수색영장을 발부받지 아니한 채 압수한 녹음파일은 사건과 관련성이 인정되지 아니하여 위법수집증거로서 증거능력이 없다고 보았다.[1)]

---

1) 2014. 1. 16. 2013도7101

2014. 6. 25. 미국 대법원에서는 체포현장에서 범인의 휴대폰에 대하여 정당한 압수수색 영장 없이는 압수수색 할 수 없다는 기념비적인 판결을 내렸다.[2] 체포현장에서 압수수색의 필요성은 체포자의 안전과 증거 보전의 필요성을 충족해야 한다. 수정헌법의 궁극적인 기준은 합리성이고, 합리성으로 위 필요성에 대하여 판단을 하면 위 요건을 만족하지 못하므로 범인의 휴대폰을 수색하기 위해서는 영장이 필요하다고 보았다. 휴대폰은 저장 용량의 대량화로 개인 사생활과 관련된 모든 개인정보를 메모리에 저장을 할 수 있다. 즉, 휴대폰은 개인 사생활의 총합체이다. 또한, 휴대폰은 네트워크로 서버에 저장되어 있는 자료를 언제, 어디서나 접속하여 볼 수 있다. 이러한 특징으로 휴대폰은 일반 물건과 달리 압수수색 영장이 필요하다고 최종 판단하였다.

본 논문에서는 디지털 증거 중 최근 여러 문제점이 제기되고 있는 휴대폰을 중심으로 증거 수집 및 분석 절차에 대하여 알아보고 그에 대한 개선방안을 제안해 본다.

첫 번째, 디지털 증거는 전통적인 유체물인 증거와 어떤 특징이 있는지 알아보겠다. 디지털 증거의 특징으로 매체독립성, 비가시성, 비가독성, 원본과 사본 구별의 곤란성, 취약성, 대량성, 전문성을 들고 있다. 더불어 디지털 증거는 혼재성이 있기 때문에 사건과 관련성 있는 파일을 압수수색 하는 것에 대한 문제가 제기된다.

두 번째, 디지털 증거 압수수색에 있어 관련성 문제를 살펴본다.

2) Riley v. California, 134 S.Ct. 2473

개정 형사소송법은 명문으로 사건과 관련된 파일에 한정하여 압수수색할 수 있도록 명시하고 있다. 우리나라 수사기관 입장에서는 적법하게 압수한 디지털 증거에서 다른 범죄사실의 증거로 사용할 수 있는 것으로 보고 있다.

하지만 대법원에서는 명백히 압수수색 영장 범죄사실 이외의 범죄사실과 관련된 증거에 대하여는 추가 압수수색 영장이 필요하다고 판단하였다. 대법원의 요구를 수사기관에서 어떻게 수용을 해야 되는지에 대하여 미국의 최신 디지털 증거 관련성 판례 및 법무부 디지털증거 매뉴얼을 통하여 바람직한 방향을 논하도록 한다.

특히, 미국의 주법원, 항소법원, 대법원의 최근 디지털 증거 관련성 개념을 알 수 있는 판결문의 주용 내용을 소개하겠다. 미국 대법원에서는 최근 체포현장에서 범인이 소지한 휴대폰에 대하여 압수수색 영장이 필요하다고 판단하였다. 일부 항소법원에서의 디지털 증거 방법제한에 대한 사례 역시 살펴보겠다.

세 번째, 휴대폰 압수수색 및 분석 절차에 대하여 알아본다. 다른 디지털 증거와 달리 개인 정보를 가장 많이 저장하고 있는 휴대폰에 대한 수사기관의 압수수색 방법을 우선 살펴본다. 휴대폰은 원격삭제 및 증거의 무결성을 확보하기 위해 전자파차폐 봉투에 넣어서 봉인하여 압수한다.

이어서 휴대폰 증거분석도구를 이용하여 플래시메모리에 저장되어 있는 모든 데이터를 추출한다. 한국 수사기관에서는 지엠디시스템의 분석도구를 사용하고 있으며, 위 도구를 통해 SQLlite DB 형태로 되어 있는 데이터를 엑셀 및 pdf 파일 형태로 분석보고서를 생성한다. 보고서 내용은 기본적인 분석정보, 메시지(카카오톡 등 포

함), 이메일, 일정, 메모, 멀티미디어, 인터넷 기록, 지도 기록 등을 보여준다.

위와 같이 휴대폰에 저장되어 있는 개인의 모든 정보에 대하여 분석보고서 형태로 일선수사팀에 인계를 한다. 디지털수사팀에서는 별도의 선별 작업을 하지 않고, 수사팀에서 내부 지침이 없는 상황에서 수사관별로 천차만별로 해당 보고서를 기록에 편철한다. 이 과정에서 사건과 관련 없는 개인의 민감한 정보까지 포함이 되며, 다른 사건과 관련된 증거 또한 수집되는 문제점에 대하여 살펴보겠다.

마지막으로 앞서 살펴본 디지털 증거 압수수색 관련성에 대하여 법원 및 수사기관의 입장 차이에 대하여 알아보겠다. 이어서, 미국 실무 및 판례의 태도를 토대로 개선방안을 제시해보겠다. 대법원의 판결 입장은 미국 실무 및 판례를 반영한 것이며, 이를 우리 수사현실에 적용하기 위해서는 압수수색 대상에 전자정보 개념이 추가 도입이 필요하다. 또한, 수사기관에서는 재차 압수수색 영장을 청구한다고 하면 수사의 효율성을 위해 2차 압수수색 영장은 사건 기록 없이 형사사법정보시스템(KICS)를 이용하여 신속하게 신청이 가능하도록 해야 될 필요성에 대하여 논해본다.

휴대폰 압수수색 및 분석 관련하여 필터링이 필요한 것을 살펴본다. 휴대폰 저장 용량의 대량화로 인해 데이터에 대한 선별 필터링은 무척 손이 많이 가고 시간이 많이 걸리는 현실이다. 또한, 사건과 필요 없는 불필요한 개인 정보 또한 볼 수 있기 때문에 수사기관에게 피의자에 대한 선입견을 가지게 할 위험이 있다. 이에 대한 개선방안으로 일선 수사팀에서 필터링을 할 수 있는 예시를 들어본다. 또한, 디지털포렌식센터에 별도의 필터링팀을 운영하여 사건과

관련된 내용에 한정하여 선별 작업을 해야 될 필요성을 논해보도록 한다.

Ⅱ. 디지털 증거에 관한 일반적 고찰

1. 디지털 증거의 개념

디지털 증거(digital evidence)는 전자 증거(electronic evidence)와 혼용 되어 사용되고 있다. 우리 나라 실무에서는 디지털 증거 개념이 주로 사용되고 있다.[3] 검찰 예규에서 정의한 디지털 증거는 범죄와 관련, 디지털 형태로 저장되거나 전송되는 것, 증거로서 가치가 있는 것이다. 외국의 경우 디지털 증거는 '이진수 형태로 저장 혹은 전송되는 법정에서 신뢰할 수 있는 정보'[4], 혹은 '디지털 형태로 저장되거나 전송되는 증거가치 있는 정보'[5] 라고 정의하고 있다.

엄격한 의미에서 전자(電子)는 디지털과 아날로그를 포함한 개념이다. 아날로그에 해당되는 증거는 녹음테이프, VHS 비디오테이프가 있으며 아날로그 증거는 디지털 증거와 다른 분석 과정이 필요하다. 또한, 법정에서 증거능력 관련하여 디지털 증거는 동일성, 무결성, 진정성이 요구되어 지는데 반해 아날로그 증거는 전문법칙에 따라 조사가 이루어진다.

---

3) 대검찰청 디지털 증거 수집 및 분석 규정, 2012.11. 6. 제3조, '디지털 증거'란 범죄와 관련하여 디지털 형태로 저장되거나 전송되는 증거로서의 가치가 있는 정보를 말한다. 경찰청/한국디지털 포렌식학회, 디지털 증거 처리 표준 가이드라인, 2006, 6면 디지털 증거라 함은 컴퓨터 또는 기타 디지털 저장매체에 저장되거나 네트워크를 통해 전송중인 자료로서 조사 및 수사업무에 필요한 증거자료를 말한다.

4) 1995년 미국, 호주, 홍콩, 영국 등 여러 국가의 법집행 관계자들을 중심으로 창설된 '컴퓨터증거에 관한 국제조직(International Organization on Computer Evidence: IOCE)

5) 1998년 미국 법무부 마약수사청, 연방수사국, 국세청 범죄수사단, 관세청, 항공우주국 등 연방기관의 증거분석 연구소들을 중심으로 구성된 '디지털증거에 관한 과학실무그룹(Scientific Working Group on Digital Evidence: SWGDE)

2. 디지털 증거의 특징

디지털 증거는 매체독립성, 비가시성, 비가독성, 원본과 사본 구별의 곤란성, 취약성, 대량성, 전문성 등의 특징을 가지고 있다.[6]

가. 매체독립성

디지털 증거는 저장 매체와 구분되어 정보 내용 자체가 증거가 되는 것이다. 예를 들어 한글 파일이 컴퓨터나 USB메모리에 저장이 되어 있더라도 같은 증거로서 가치를 가지고 있다.

하지만, 만약 해당 한글 파일의 작성일자가 사건에 있어 쟁점이 되는 경우를 생각해 보자. 피의자는 악의적으로 시간 정보 변경 프로그램[7]을 이용하여 한글 파일의 맥타임[8]을 변경을 했을 경우, 한

---

6) 디지털 포렌식 관련 학위 논문 대부분을 보면 위와 같은 대지털 증거의 특징을 들고 있다.

7) 맥타임 변조 프로그램은 http://www.softwareok.com/ 사이트 등에서 쉽게 구할 수 있다.

8) 맥타임은 MAC TIME의 약자로, Modification time(수정시간), Access time(접근시간), Creation time(생성시간)의 약자이다. 맥타임은 포렌식에서 중요한 위치를 가지고 있지만, 윈도우 파일시스템(FAT, NTFS)에서 맥타임이 변경되는 사례가 많이 있어 획일적으로 맥타임에 맹신하면 안된다. 맥타임과 더불어 고찰해보야 할 대상은 한글문서나 MS워드는 복합문서로, 해당 문서 파일 내부에 별도의 시간 정보를 기록을 한다. 파일시스템으로 보이는 파일의 맥타임은 파일의 복사 등으로 파일의 수정, 생성 시간 등이 변동이 되지만, 위 복합문서 내부에 있는 최초 파일 생성 시간은 파일 복사로 변동이 되지 않는다. 그나마, 위 복합문서 내부에 있는 시간 정보가 정확하고 이를 기반으로 사건에 적용을 하는 편이 보다 정확한 값을 나타내준다.
예를 들어, 한글과컴퓨터에서 배포한 한글문서 5.0 포맷을 보면, \005HwpSummaryInfomation 스트림에는 흔글 메뉴의 "파일-문서 정보-문서 요약"에서 입력한 내용이 아래와 같이 저장이 된다. 아래 내용중 중요한 것은 Author(저자, 컴퓨터 계정 정보를 알 수 있음), Create Time(파일의 최초 생성일자), Last saved Time(최종 수정시간).

글 파일 자체만 압수수색해서는 사건 실마리가 풀리지 않는다. 이때, 해당 파일을 변조한 컴퓨터 등에 저장되어 있는 변조프로그램 설치여부, 레지스트리 정보 등을 분석하여 피의자가 어떠한 방식으로 문서에 대한 시간정보를 변경했는지 찾아야 한다.

나. 비가시성·비가독성

디지털 증거는 0, 1의 이진수의 조합으로 이루어졌고, 위와 같은 디지털 증거의 내용을 확인하기 위해서는 해당 파일의 응용프로그램이 필요하다. 물론, 디지털증거 분석프로그램인 인케이스, FTK[9]

Name	Property ID string	Property ID	VT type
Title	PIDSI_TITLE	0x00000002	VT_LPSTR
Subject	PIDSI_SUBJECT	0x00000003	VT_LPSTR
Author	PIDSI_AUTHOR	0x00000004	VT_LPSTR
Keywords	PIDSI_KEYWORDS	0x00000005	VT_LPSTR
Comments	PIDSI_COMMENTS	0x00000006	VT_LPSTR
Last Saved By	PIDSI_LASTAUTHOR	0x00000008	VT_LPSTR
Revision Number	PIDSI_REVNUMBER	0x00000009	VT_LPSTR
Last Printed	PIDSI_LASTPRINTED	0x0000000B	VT_FILETIME (UTC)
Create Time/Date((*))	PIDSI_CREATE_DTM	0x0000000C	VT_FILETIME (UTC)
Last saved Time/Date((*))	PIDSI_LASTSAVE_DTM	0x0000000D	VT_FILETIME (UTC)
Number of Pages	PIDSI_PAGECOUNT	0x0000000E	VT_I4
Date String(User define)	*HWPPIDSI_DATE_STR*	*0x00000014*	*VT_LPSTR*
Para Count(User define)	*HWPPIDSI_PARACOUNT*	*0x00000015*	*VT_I4*

9) 검찰은 최초 디지털증거분석용 프로그램으로 파이널데이터사를 통해서 'DEAS' 프로그램을 제작하여 사용을 하였다. 위 프로그램을 이용하여 압수수색과 증거분석에 모두 이용을 하였다. 2006년경 본 프로그램의 한계가 있어, 검찰은 가이던스소프트웨어사의 Encase(인케이스) 증거통합분석 프로그램을 구입하여 증거분석에 이용하였다. 위 인케이스는 일심회 판결문에 등장을 하고, 미국 법정에서 인증이 이루어진 프로그램이다. 증거분석을 하기 위해서는 하나의 프로그램만 사용해서는 안되고 최소한 2~3개이 프로그램을 이용하여 서로 결과값을 비교 분석해야 한다. 그래서, 검찰은 미국 액세스데이터사로부터 FTK 증거통합분석프로그램을 구입하여 인케이스와 같이 증거분석용으로 사용을 하고 있다. 인케이스에서 제공하는 증거 이미지 해시값은 법정에서 무결성을 입증하는데 사용되고 있으

등은 대부분의 파일을 지원하여 응용프로그램이 필요하지 않을 수도 있다. 이러한 특징으로, 사건과 관련성이 있는 파일인지 확인하기 위해서는 해당 파일을 직접 열어서 확인할 수 밖에 없다.

다. 원본과 사본 구별의 곤란성

디지털 증거는 수회 반복하여 복사를 해도 원본과 같은 결과물을 생성해준다. 아날로그 녹음테이프 같은 경우 복사를 여러 번 할 때마다 음질 등에서 차이가 있는 것과 비교가 된다. 비록 원본과 사본의 구별 실익이 크지 않더라도, 한글 문서 파일이나 워드로 작성된 문서 파일 같은 경우 파일이 다른 저장 장치로 복사를 할 경우 맥타임 등에서 차이가 나는 것으로 원본이나 사본 여부를 따져 볼 수도 있다.

라. 취약성

디지털 증거는 위조, 변조 등이 용이한 특징이 있다. 이러한 특징은 주로 피고인 측 변호인이 주장하는 경우가 많이 있다. 피고인은 어떻게 해서든 해당 문서는 자신이 작성을 한 것이 아니라 수사기관에서 자신을 처벌하기 위해 고의로 작성을 한 것이라고 주장을

며, 검찰의 대부분 증거사본은 인케이스를 이용하여 생성되고 있는 실정이다. 위 프로그램 모두 미국 美국립표준기술원(NIST)의 CFTT(Computer Forensic Tool Testing)에서 기록의 무결성 검증 기능테스트를 통과한 제품이다. 2014년 기준 CFTT의 삭제파일 복구프로그램 중 기능테스트를 통과한 제품은, ILooKIX v2.2.3.151, September 2014 , The Sleuth Kit (TSK) 3.2.2 / Autopsy 2.24, July 2014, X-Ways Forensics Version 16.0 SR-4, July 2014, SMART for Linux Version 2011-02-02 (Revised), June 2014, FTK Version 3.3.0.33124, Revised June 2014, EnCase Version 6.18.0.59, Revised June 2014.

한다. 하지만, 대부분 디지털 증거 관련 무결성(chain of custody)[10] 이 입증이 되면 변호인 주장은 기각이 된다. 미국에서도 위와 같은 주장에 대하여 대부분 법원에서 인정을 해주지 않고 있다.

마. 대량성

최근 저장기술의 발전으로 물리적으로 아주 작은 저장매체에도

---

10) 디지털증거에 관한 과학실무그룹(Scientific Working Group on Digital Evidence: SWGDE)에서는, 무결성을 확보하기 위해서는 아래와 같은 절차를 거쳐야 한다고 설명하고 있다.

In order to ensure that digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system. Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and use broadly accepted procedures, equipment, and materials.
All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.
Agency management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness.
Procedures used must be generally accepted in the field or supported by data gathered and recorded in a scientific manner.
The agency must maintain written copies of appropriate technical procedures
The agency must use hardware and software that is appropriate and effective for the seizure or examination procedure.
All activity relating to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony.
Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner.

방대한 분량의 정보를 저장할 수 있게 되었다. 또한 개인이 사용하는 컴퓨터나 디지털 저장매체일지라도 갖가지 종류의 응용프로그램에 의해 생성된 수많은 형태의 자료가 저장되어 있는 경우가 많다. 특히 여러 사람이 공동으로 이용하는 서버의 경우에는 하나의 저장매체 또는 시스템인 경우라도 압수대상이 되는 특정인의 자료만 저장 또는 전송되는 것이 아니라 범죄와 관계없는 수많은 사람들의 데이터가 저장 또는 전송되는 것이 통상적이다. 따라서 증거수집의 범위와 관련된 법적문제가 발생할 수 있다. 또한, 대량의 데이터가 대규모로 집적되어 저장, 처리, 전송되는 만큼 저장된 물리적 저장매체를 압수하여 분석하는 데에는 강력한 성능을 가진 시스템이 필요하고 장기간의 시간과 전문적인 지식이 소요되는 경우가 발생한다.[11]

바. 전문성

대검찰청에서는 원칙직으로 디지털증거 분석은 일선 수사기관에서 직접 할 수 없고, 모든 디지털 증거 관련하여 소속 검찰청을 관할하는 디지털포렌식 센터에 증거 분석을 의뢰해야 한다. 가장 큰 이유는 디지털 증거는 무결성을 확보하지 않으면 법정에서 증거로 사용될 수 없기 때문이다. 검찰 및 경찰에서는 디지털전문 담당 부서가 별도로 있으며 해당 부서에 근무하는 수사관은 디지털 증거 관련 교육을 이수하였고 필요할 경우 법정에 나가 증인으로 증언을 해야 한다.[12] 일심회 판결에서도 '조작자의 전문적 기술능력 등이

11) 고려대학교 산학협력단, "외국판례에 나타난 디지털증거 수집·분석·보존 과정에서의 무결성 논란에 비추어 본 디지털 증거의 활용방안", 대검찰청, (2006), 6면.
12) 한국포렌식학회에서 주관하고 있는 국가 공인 디지털포렌식전문가 1, 2급 자격시험,

갖추어질 것 등을 제시하였다.[13] 미국 일부 법원에서 압수 방법 제한 방식으로(protocol) 위 전문성을 가진 분석관에 의하여 최초 디지털 증거가 수색이 되어야 한다는 조건을 들었다.[14]

사. 혼재성

위에서 살펴본 디지털 증거는 지금까지 대부분의 논문에서 언급되어진 특징이다. 기존 연구 논문에서는 대량성이란 특징 안에 혼재성을 언급하고 있다. 하지만, 혼재성이란 특징은 별도로 구분되어 설명되어야 한다. 왜냐하면, 디지털 증거가 대량의 저장매체에 보관되어 있다는 점과 그 정보 중에 사건과 관련이 없는 것이 같이 저장이 되어 있다는 것은 같은 개념이 아니다.

2012년 형사소송법이 개정이 된 주된 이유는 신정아 사건에서 검찰이 컴퓨터에 저장되어 있던 이메일을 복원한 것이 언론에 회자가

AccessData社에서 운영하고 있는 디지털포렌식 전문 자격인 ACE(AccessData Certified Examiner)자격증, 가이던스소프트웨어의 ENCE(EnCase Certified Examiner) 등의 자격으로 1차적으로 전문성을 판단할 수 있다. 추가적으로 위 자격증과 더불어 관련 분야 근무 경력, 교육 이력 등을 토대로 전문성 있는 분석관인지 알 수 있다.

13) 서울중앙지방법원 2007. 4. 16. 선고 2006고합1365판결 ; 서울고등법원 2007. 8. 16. 선고 2007 노 929 ; 대법원 2007. 12. 13. 선고 2007도7257

14) United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010), The warrant also contained significant restrictions on how the seized data were to be handled. These procedures were designed to ensure that data beyond the scope of the warrant would not fall into the hands of the investigating agents. Thus, the initial review and segregation of the data was not to be conducted by the investigating case agents but by "law enforcement personnel trained in searching and seizing computer data ('computer personnel')," whose job it would be to determine whether the data could be segregated on-site. These computer personnel not the case agents were specifically authorized to examine all the data on location to determine how much had to be seized to ensure the integrity of the search.

되었고, 일반 시민들 입장에서는 웹메일로 읽어 본 메일 또한 검찰이 복원하면 개인 사생활에 너무 큰 피해가 가는 우려를 보였다. 하지만, 신정아 사건에서 이메일을 복원했다는 것은 해당 컴퓨터에서 아웃룩 이메일(확장자 dbx, pst)을 복구한 것이다. 웹메일을 읽어 본 것에 대해서는 하드디스크 저장 장치에 기록이 되지 않고 컴퓨터가 활성 상태에서만 메모리에 잠시간 저장이 될 뿐이다. 하지만, 그렇다고 해도 아웃룩을 통하여 외부 웹메일을 연동하여 같이 사용을 했으면, 그 이메일에는 사건과 관련 없는 수 많은 개인 적으로 민감한 메일이 많이 있을 것이고, 그것을 그대로 수사기관에서 열람할 수 있다는 것은 개인 입장에서는 기분 좋은 일이 아닐 것이다.

이러한 우려를 불식시키기 위하여 개정된 형사소송법에서는 사건과 관련된 정보에 한정하여 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다고 개정되었다.

Ⅲ. 디지털 증거 압수수색에 있어 관련성 문제

1. 디지털 증거의 관련성 개념

가. 형사소송법 규정

2011. 7. 18. 형사소송법 일부개정이 되었고, 개정이유는 수사기관의 책임감을 높이고, 피의자·피고인의 인권침해를 최소화하며, 수사현실과 법률규정이 부합하도록 현행법을 정비하는 한편, 누구든지 확정된 형사사건의 판결서와 증거목록 등을 인터넷 등 전자적 방법으로도 열람 및 등사할 수 있도록 함으로써 판결서 등에 대한 접근성을 높여 재판의 공개 원칙이 실질적으로 보장되도록 하려는 것이다.[15)]

압수수색과 관련 개정내용은 ① 법원의 압수·수색의 요건에 피고사건과의 관련성을 추가함 ② 정보저장매체등에 관한 압수의 범위와 방법을 명시하고, 정보주체에게 해당 사실을 알리도록 하며, 영장에는 작성기간을 기재토록 명시하는등 전기통신관련 압수·수색제도를 보완 ③ 수사기관의 압수·수색·검증의 요건에 피고사건고의 관련성과 피의자가 죄를 범하였다고 의심할만한 정황이 있을 것을 추가하였다.

제106조(압수)
① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물

15) 2011. 7. 18. 형사소송법 일부개정 이유

건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다. <개정 2011.7.18>

② 법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다.

③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다. <신설 2011.7.18>

④ 법원은 제3항에 따라 정보를 제공받은 경우 「개인정보 보호법」 제2조제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다. <신설 2011.7.18>

제109조(수색)

① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 피고인의 신체, 물건 또는 주거, 그 밖의 장소를 수색할 수 있다. <개정 2011.7.18>

② 피고인 아닌 자의 신체, 물건, 주거 기타 장소에 관하여는 압수할 물건이 있음을 인정할 수 있는 경우에 한하여 수색할 수 있다.

제114조(영장의 방식)

① 압수·수색영장에는 피고인의 성명, 죄명, 압수할 물건, 수색할 장소, 신체, 물건, 발부연월일, 유효기간과 그 기간을 경과하면 집행에 착수하지 못하며 영장을 반환하여야 한다는 취지 기타

대법원규칙으로 정한 사항을 기재하고 재판장 또는 수명법관이 서명날인하여야 한다. 다만, 압수·수색할 물건이 전기통신에 관한 것인 경우에는 작성기간을 기재하여야 한다. <개정 2011.7.18>

② 제75조제2항의 규정은 전항의 영장에 준용한다.

제118조(영장의 제시)

압수·수색영장은 처분을 받는 자에게 반드시 제시하여야 한다.

제120조(집행과 필요한 처분)

① 압수·수색영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다.

② 전항의 처분은 압수물에 대하여도 할 수 있다.

제121조(영장집행과 당사자의 참여)

검사, 피고인 또는 변호인은 압수·수색영장의 집행에 참여할 수 있다.

제122조(영장집행과 참여권자에의 통지)

압수·수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다.

제129조(압수목록의 교부)

압수한 경우에는 목록을 작성하여 소유자, 소지자, 보관자 기타 이에 준할 자에게 교부하여야 한다.

제131조(주의사항)

압수물에 대하여는 그 상실 또는 파손 등의 방지를 위하여 상

당한 조치를 하여야 한다.

제133조 (압수물의 환부, 가환부)

① 압수를 계속할 필요가 없다고 인정되는 압수물은 피고사건 종결 전이라도 결정으로 환부하여야 하고 증거에 공할 압수물은 소유자, 소지자, 보관자 또는 제출인의 청구에 의하여 가환부할 수 있다.

② 증거에만 공할 목적으로 압수한 물건으로서 그 소유자 또는 소지자가 계속 사용하여야 할 물건은 사진촬영 기타 원형보존의 조치를 취하고 신속히 가환부하여야 한다.

나. 개정 전 형사소송법상 압수수색 청구 요건

개정 전 형사소송법상에서도 명문에는 규정을 하지 않았지만 당연히 범죄 혐의가 있는 경우 범죄수사에 필요한 경우 압수수색 영장을 청구하였다. 여기서, 범죄 혐의 정도는 체포·구속에 비하면 범죄혐의가 정도가 낮은 것으로 해석을 하였다. 그리고, 수사에 필요한 경우 압수수색을 할 수 있다. 여기서 필요성의 개념에 이미 관련성과 비례성이 포함이 되어 있는 것으로 다수설은 해석을 한 것으로 보고 있었다. 판례는 필요성, 상당성, 비례성을 들고 있다.[16]

16) 대법원 2004. 3. 23. 선고 2003모126 결정
형사소송법 제215조 에 의하면 검사나 사법경찰관이 범죄수사에 필요한 때에는 영장에 의하여 압수를 할 수 있으나, 여기서 '범죄수사에 필요한 때'라 함은 단지 수사를 위해 필요할 뿐만 아니라 강제처분으로서 압수를 행하지 않으면 수사의 목적을 달성할 수 없는 경우를 말하고, 그 필요성이 인정되는 경우에도 무제한적으로 허용되는 것은 아니며, 압수물이 증거물 내지 몰수하여야 할 물건으로 보이는 것이라 하더라도, 범죄의 형태나 경중, 압수물의 증거가치 및 중요성, 증거인멸의 우려 유무, 압수로 인하여 피압수자가 받을 불이익의 정도 등 제반 사정을 종합적으로 고려하여 판단해야 할 것이다.
원심결정 이유에 의하면 원심은, 검사가 이 사건 준항고인들의 폐수무단방류 혐의가 인정된다는 이유로 준항고인들의 공장부지, 건물, 기계류 일체 및 폐수운반차량 7대에 대

1) 범죄 혐의

압수・수색의 경우에도 체포, 구속과 같이 범죄혐의가 있어야 한다. 다만 체포, 구속에 관하여는 “죄를 범하였다고 의심할 만한 상당한 이유”를 요건으로 요구하면서(법 제200조의2 제1항, 제201조 제1항), 압수・수색의 경우에는 이를 명시하지 않은 채 “범죄수사에 필요한 경우”(법 제215조 제1항, 제2항)라고만 하고 있고, 수사과정에서 통상 체포 구속에 앞서 범죄혐의 유무를 확인하기 위하여 압수수색이 이루어지는 점 등을 비추어 볼 때 체포・ 구속에 비하여 범죄혐의의 정도가 낮아도 무방하다고 해석된다.[17]

2) 압수・수색의 필요성

범죄수사에 필요한 때에 판사가 발부한 영장에 의하여 압수・수색할 수 있다(법 제215조 제1항, 제2항). 압수・수색의 필요성은 범죄의 형태와 경중, 대상물의 증거가치, 중요성 및 멸실의 염려, 처분을 받는 자의 불이익의 정도 등 제반사정을 고려하여 결정하여야 한다.[18]

다. 개정 형사소송법 취지

위와 같이 기존 압수수색 관련하여 필요성, 범죄 혐의가 있는 경

하여 한 압수처분은 수사상의 필요에서 행하는 압수의 본래의 취지를 넘는 것으로 상당성이 없을 뿐만 아니라, 수사상의 필요와 그로 인한 개인의 재산권 침해의 정도를 비교형량해 보면 비례성의 원칙에 위배되어 위법하다고 판단하였는바, 기록과 위의 법리에 비추어 살펴보면, 원심의 위와 같은 판단은 정당한 것으로 수긍이 가고, 거기에 주장과 같은 압수의 요건에 관한 법리오해의 위법이 없다.

17) 위재민, “형사절차법”, 대검찰청 내부 게시판, 61면

18) 위재민, “형사절차법”, 대검찰청 내부 게시판, 61면

우만 압수수색을 청구할 수 있었고, 필요성 개념에 사건과의 관련성이 포함이 된 것으로 해석을 하고 있었고, 실무상 사건과 아무런 관련 없는 증거를 압수수색 하는 것은 수사기관 및 영장 발부기관인 법원에서 전혀 생각할 수 없었다. 하지만, 굳이 개정형사소송법에서 관련성 개념을 명문에 추가한 것은 기존 수사기관의 압수수색에 있어 사건과 관련 없는 증거가 광범위하게 압수가 되고 있는 현실을 반영한 것임에는 자명하다.

특히, 2006년경 검찰 및 경찰에서는 디지털수사 예규 및 가이드라인을 자체 정립하여 디지털 기기에 대한 압수수색을 광범위하게 실시하였다. 당시 디지털 증거 압수수색은 원본 압수가 원칙이고, 하드디스크 등을 압수하면 즉시 해당 증거물을 사본 작성 후 분석을 하였다. 경찰뿐만 아니라 검찰에서도 수사 파트와 디지털 포렌식 파트는 구분되어 일을 각각 진행을 했다. 디지털 포렌식 팀은 수사 파트에서 요구하는 사건과 관련이 있는 문서 파일 등을 검색하기 위하여 수사검색시스템을 제작하여 키워드 검색을 하였다.[19]

디지털 포렌식 수사관이 사건과 관련이 있는 문서파일만 필터링하여 일선 수사팀에 전달을 하면 가장 이상적으로 사건 관련자의 인권 보장 등에 기여를 할 수 있을 것이다. 2006년 당시 하드디스크는 보통 100~300GB 용량을 사용하였고, 업무용으로 사용된 증거물

19) 검찰에서는 IQS(수사질의어시스템) 프로그램을 외부 업체 용역을 통하여 제작하였다. 포렌식 수사관은 디지털 증거에서 모든 문서파일, 이메일 등을 추출하여 DVD에 저장을 하고, 위 IQS 검색시스템은 CD로 사본하여 수사팀에 배포한다. 수사팀에서는 DVD에 있는 문서파일 등을 수사관 컴퓨터에 백업을 하고, IQS CD를 이용해서 문서 검색 등을 한다. 이런 시스템에서 보여지는 한계는 디지털포렌식 수사관이 사건과 관련이 있는 문서파일을 필터링하여 관련 있는 파일만 DVD에 저장을 할 수 없었고, 일단 해당 증거물에 저장되어 있는 모든 문서파일을 업로드한 것이 문제가 된다. 물론, 디지털 수사 인력의 한계와 더불어 1개의 하드디스크에 저장되어 있는 문서파일 용량이 크기 때문에 사건과 관련이 있는 파일을 한정하는 것은 역부족이다.

같은 경우 문서파일, 이메일 등을 추출하면 대략 30~50GB 정도 나오게 된다. 이러한 문서파일에 대하여 사건 담당 포렌식 수사관 1명이 수사팀에서 인계한 범죄사실을 참고하여 문서파일을 추출하는 것은 시간상 역부족이었다.

그리고, 디지털포렌식 수사관이 임의로 어떤 파일은 사건과 관련성이 있고 어떤 파일은 사건과 전혀 관련성이 없다고 판단하는 것은 무척 어렵다. 시간 제약상 파일의 모든 내용을 살펴 볼 수 없기 때문에 문서 파일의 제목이나 수사검색시스템을 통하여 검색을 하더라도 사건과 관련성이 있는 것을 명확히 구분하는 것은 어렵다.

2007. 10. 30. 서울서부지검에서는 전 대통령 비서실 정책실장 변양균과 전 동국대학교 조교수 신정아를 뇌물수수, 제3자뇌물수수, 업무방해 등 혐의로 구속기소하였다. 당시, 수사팀에서 언론 중간발표 내용을 보면 50여 곳을 압수수색하고 총 7.71.TB(테라바이트) 분량의 디지털 증거자료를 분석하였다. 그리고, 신정아의 주거지에서 입수한 PC에서 복구한 이메일 파일, PC에서 추출·복구한 휴대폰 통신자료 등에서도 변양균 이외에 친분 있는 고위층은 전혀 확인되지 아니하였다.[20] 여기서 세인들의 관심을 가졌던 부분은 신정아 주거지에서 압수한 PC에서 검찰이 어떤 이메일을 복구한 것인지였다. 당시 매일 언론에 사건이 보도가 되었고 디지털포렌식이란 것이 조명을 받게 되었다.

하지만, 일각에서는 검찰에서 개인의 이메일을 복구하게 되면 그 이메일에는 사건과 관련이 있는 것이 있을 수 있지만, 사건과 관련이 없이 제 3자와 서로 주고받은 이메일이 많이 있을 것이고, 수사기관에서 사건과 관련이 없는 이메일을 보는 것에 반감을 가지게

20) 2007.10.30. 신정아 변양균 사건 관련 중간수사 결과 발표자료, 서울서부지방검찰청.

되었다. 이런 반감은 당시 법제사법위원 일부가 직접 검찰 디지털포렌식 센터에 방문하여 검찰의 증거 분석 절차에 대하여 살펴보기까지 하였다.

이후, 법제사법위원회 박영선 의원을 주축으로 압수수색 영장에 사건과 관련성이 있는 자료만 압수하여 개인의 인권보호에 기여하는 방향으로 압수수색 영장이 개정이 되었다.

2. 우리나라 판례에 있어서 관련성 검토

가. 2009모1190 결정(2011. 5. 26. 준항고기각결정에 대한 재항고)

1) 결정요지

> 전자정보에 대한 압수·수색영장의 집행에 있어서는 원칙적으로 영장 발부의 사유로 된 혐의사실과 관련된 부분만을 문서 출력물로 수집하거나 수사기관이 휴대한 저장매체에 해당 파일을 복사하는 방식으로 이루어져야 하고, 집행현장의 사정상 위와 같은 방식에 의한 집행이 불가능하거나 현저히 곤란한 부득이한 사정이 존재하더라도 그와 같은 경우에 그 저장매체 자체를 직접 혹은 하드카피나 이미징 등 형태로 수사기관 사무실 등 외부로 반출하여 해당 파일을 압수·수색할 수 있도록 영장에 기재되어 있고 실제 그와 같은 사정이 발생한 때에 한하여 예외적으로 허용될 수 있을 뿐이다. 나아가 이처럼 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄 혐의 관련 전자

정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보아야 한다. 따라서 그러한 경우의 문서출력 또는 파일복사의 대상 역시 혐의사실과 관련된 부분으로 한정되어야 함은 헌법 제12조 제1항, 제3항, 형사소송법 제114조, 제215조의 적법절차 및 영장주의의 원칙상 당연하다. 그러므로 수사기관 사무실 등으로 옮긴 저장매체에서 범죄 혐의와의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이 된다.

한편 검사나 사법경찰관이 압수·수색영장을 집행함에 있어서는 자물쇠를 열거나 개봉 기타 필요한 처분을 할 수 있지만 그와 아울러 압수물의 상실 또는 파손 등의 방지를 위하여 상당한 조치를 하여야 하므로(형사소송법 제219조, 제120조, 제131조 등), 혐의사실과 관련된 정보는 물론 그와 무관한 다양하고 방대한 내용의 사생활 정보가 들어 있는 저장매체에 대한 압수·수색영장을 집행함에 있어서 그 영장이 명시적으로 규정한 위 예외적인 사정이 인정되어 그 전자정보가 담긴 저장매체 자체를 수사기관 사무실 등으로 옮겨 이를 열람 혹은 복사하게 되는 경우에도, 그 전체 과정을 통하여 피압수·수색 당사자나 그 변호인의 계속적인 참여권 보장, 피압수·수색 당사자가 배제된 상태에서의 저장매체에 대한 열람·복사 금지, 복사대상 전자정보 목록의 작성·교부 등 압수·수색의 대상인 저장매체 내 전자정보의 왜곡이나 훼손과 오·남용 및 임의적인 복제나 복사 등을 막기 위한 적

절한 조치가 이루어져야만 그 집행절차가 적법한 것으로 될 것이다.

원심결정 이유를 기록에 비추어 살펴보면, 수사기관이 이 사건 압수·수색영장을 집행함에 있어 그 영장이 허용한 바와 같은 사유로 이 사건 저장매체 자체를 영장 기재 집행장소에서 수사기관 사무실로 가져가 그곳에서 저장매체 내 전자정보파일을 다른 저장매체로 복사하였는데, 그 과정 내내 피압수·수색 당사자의 직원들과 변호인들의 참여가 허용된 사실, 위 당사자 측의 참여하에 이루어진 이 사건 전자정보파일의 복사에 있어 그 대상을 영장에 기재된 혐의사실의 일시로부터 소급하여 일정 시점 이후에 열람된 파일들로 제한한 사실, 이러한 압수·수색영장의 집행방법과 관련하여 당사자 측은 위 소급 복사하는 파일 열람시점에 관한 의견만 제시하였을 뿐, 범죄 혐의와의 관련성에 관한 별도의 이의나 저장매체의 봉인 요구 등 절차상 이의를 제기하지 않고 오히려 위와 같은 방법으로 수사기관이 대상 전자정보파일을 복사하여 담아 둔 저장매체 2개 중 하나를 수령하였을 뿐만 아니라 위 영장의 집행일인 2009. 7. 3. 당일이 아닌 2009. 7. 6.에야 비로소 이 사건 준항고를 제기한 사실 등을 알 수 있다.

앞서 본 법리와 위 인정 사실에 의하면, 수사기관이 이 사건 저장매체 내 전자정보에 대한 압수·수색영장을 집행함에 있어 저장매체 자체를 수사기관 사무실로 옮긴 것은 영장이 예외적으로 허용한 부득이한 사유의 발생에 따른 것으로 볼 수 있고, 나아가 당사자 측의 참여권 보장 등 압수·수색 대상물건의 훼손이나 임의적 열람 등을 막기 위해 법령상 요구되는 상당한 조치가

이루어진 것으로 볼 수 있으므로 이 점에 있어 절차상 위법이 있다고는 할 수 없다. 다만 수사기관 사무실에서 저장매체 내 전자정보를 파일복사함에 있어서 당사자 측의 동의 등 특별한 사정이 없는 이상 관련 파일의 검색 등 적절한 작업을 통해 그 대상을 이 사건 범죄 혐의와 관련 있는 부분에 한정하고 나머지는 대상에서 제외하여야 할 것이므로, 영장의 명시적 근거가 없음에도 수사기관이 임의로 정한 시점 이후의 접근 파일 일체를 복사하는 방식으로 8,000여 개나 되는 파일을 복사한 이 사건 영장집행은 원칙적으로 압수·수색영장이 허용한 범위를 벗어난 것으로서 위법하다고 볼 여지가 있다.

그런데 범죄사실 관련성에 관하여 명시적인 이의를 제기하지 아니한 이 사건의 경우, 당사자 측의 참여하에 이루어진 위 압수·수색의 전 과정에 비추어 볼 때, 수사기관이 영장에 기재된 혐의사실의 일시로부터 소급하여 일정 시점 이후의 파일들만 복사한 것은 나름대로 혐의사실과 관련 있는 부분으로 대상을 제한하려고 노력을 한 것으로 보이고, 당사자 측도 그 조치의 적합성에 대하여 묵시적으로 동의한 것으로 봄이 상당하므로, 결국 이 사건 범죄 혐의와 관련 있는 압수·수색의 대상을 보다 구체적으로 제한하기 위한 수사기관의 추가적인 조치가 없었다 하여 그 영장의 집행이 위법하다고 볼 수는 없다

2) 평가

동 대법원 결정은 2011. 7. 18. 형사소송법 개정에 많은 영향을 준 것으로 학계에서 보고 있다. 이숙연 판사는 전자정보는 그 취약성과

대량성 등으로 인하여, 압수수색영장을 발부받아 집행에 이르는 경우에도, 포괄적 압수수색의 문제가 발생하게 되며 당사자의 정보자기결정권을 어떻게 보호할 것인가의 문제가 발생한다. 대법원의 동 결정은 이러한 난제들에 대한 고민과 결단을 담은 기념비적인 판결이라고 평가를 하였다.[21]

하지만, 수사기관 입장에서는 위 재항고 결정에 대하여 난색을 표시하였다. 전승수 검사는 위 결정과 관련하여, 압수수색 집행과정을 지나치게 확장하고, 영장의 집행종료시점을 확정하지 아니하여 참여권을 지나치게 보장하는 문제점을 제기하였다. 이어서, 디지털 증거는 유체물과 달리 대량성, 네트워크 관련성 등의 특징을 가지고 있다. 유체물을 전제로 하는 압수수색절차를 디지털 증거에 그대로 적용하기 어렵고, 신설된 형사소송법 제106조 제3항과 제4항만으로는 기본권 보호나 수사의 목적을 모두 충족시킬 수 없다. 따라서 종래의 압수수색절차를 기본으로 하되, 디지털 증거의 특성과 기술 발전 가능성을 감안하여 개인의 기본권을 보호하면서도 실무에서 적절하게 증거를 확보할 수 있는 새로운 절차가 요청된다고 보고 있다.[22]

나. 2013도7101판결(공직선거법위반, 정치자금법위반)

1) 공소사실 및 압수수색 영장 기재 내용[23]

○ 피의자 : 甲

21) 이숙연, “전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여”, 헌법학연구 제18권 제1호, 2012. 3월호
22) 전승수, “디지털 정보에 대한 압수수색영장의 집행”, 법조, 2012. 7월호, 273면
23) 오기두, “관련성 없는 휴대폰 녹음 파일 압수와 위법수집증거”, 법률신문 2013. 3. 4.자, 13면

○ 죄명 : 알선뇌물공여
○ 압수할 물건 : 참고인 乙 소유의 휴대전화(휴대전화, 스마트폰 등), 태블릿PC(아이패드, 갤럭시탭 종류) 및 저장된 정보
○ 범죄사실 및 압수를 필요로 하는 사유 : 피의자 甲은 2012. 3. 15. 공무원인 참고인 乙에게, 역시 공무원인 A에게 그 A의 직무와 관련한 청탁과 함께 전달해 달라는 부탁을 하고 서울역 구내 어느 한식당에서 1억 원을 주어 A의 직무에 속한 사항의 알선에 관하여 乙에게 뇌물을 공여하였다.

영장담당 판사로부터 위와 같은 기재가 있는 압수수색영장을 발부받은 수사관은 참고인 乙의 주거지에서 乙의 휴대폰을 압수하였다. 그 휴대폰에는 乙가 丙와의 대화내용을 녹음한 파일이 있다. 대화내용 중에는 乙이 A에게 이미 로비를 하였다는 말 등 甲-乙간의 금품수수를 추단케 할 만한 내용이 있다. 나아가 다음과 같은 乙-丙간 뇌물요구 및 뇌물공여 약속 범행을 인정케 하는 내용도 녹음되어 있다.

검사는 乙의 휴대폰에 있던 녹음파일의 음성내용을 근거로 乙와 丙을 수사하여 위 공소사실로 기소하였다. 그것을 입증할 증거로 위 녹음파일의 녹취록을 제출하고 있다.

2) 판결요지

수사기관이 피의자 甲의 공직선거법 위반 범행을 영장 범죄사실로 하여 발부받은 압수·수색영장의 집행 과정에서 乙,丙사이의 대화가 녹음된 녹음파일(이하 '녹음파일'이라 한다)을 압수하여 乙,丙의 공직선거법 위반 혐의사실을 발견한 사안에서, 압수·수색영장에 기재된 '피의자'인 甲이 녹음파일에 의하여 의심되는 혐의사실과 무관한 이상, 수사기관이 별도의 압수·수색영장을 발부받지 아니한 채 압수한 녹음파일은 형사소송법 제219조 에

의하여 수사기관의 압수에 준용되는 형사소송법 제106조 제1항이 규정하는 '피고사건'내지 같은 법 제215조 제1항 이 규정하는 '해당 사건'과 '관계가 있다고 인정할 수 있는 것'에 해당하지 않으며, 이와 같은 압수에는 헌법 제12조 제1항 후문,제3항 본문이 규정하는 영장주의를 위반한 절차적 위법이 있으므로, 녹음파일은 형사소송법 제308조의2 에서 정한 '적법한 절차에 따르지 아니하고 수집한 증거'로서 증거로 쓸 수 없고, 그 절차적 위법은 헌법상 영장주의 내지 적법절차의 실질적내용을 침해하는 중대한 위법에 해당하여 예외적으로 증거능력을 인정할 수도 없다고 한 사례.

3) 이유 요지

가.피고인 1・피고인 7사이의 대화를 녹음한 녹음파일(이하 '이 사건 녹음파일'이라 한다)및 그에 기하여 수집된 증거들의 증거능력에 대하여

(1)이 사건 녹음파일의 증거능력에 관하여

(가)원심은 부산지방검찰청 검사가 2012.8.3.부산지방법원으로부터 압수・수색영장(이하 '이 사건 영장'이라 한다)을 발부받았는데,이 사건 영장에 피의자는 '피고인 2',압수할 물건은 '피고인 1 등이 소지하고 있는 휴대전화(휴대전화,스마트폰)등',압수・수색할 장소는 '피고인 1의 주거지 등',영장 범죄사실은 '피의자는 공천과 관련하여,2012.3.15.및 3.28.공소외 1에게 지시하여 ○○○당

공천심사위원인 공소외 13등에게 거액이 든 돈 봉투를 각 제공하였다 등'으로 각 기재되어 있는 사실,이에 따라 부산지방검찰청 수사관이 피고인 1의 주거지에서 그의 휴대전화를 압수하고 이를 부산지방검찰청으로 가져온 후 그 휴대전화에서 추출한 전자정보를 분석하던 중 피고인 1과 피고인 7사이의 대화가 녹음된 이 사건 녹음파일을 통하여 위 피고인들에 대한 공직선거법 위반의 혐의점을 발견하고 수사를 개시하였으나,위 피고인들로부터 이 사건 녹음파일을 임의로 제출받거나 새로운 압수수색영장을 발부받지 아니하였던 사실 등을 각 인정한 다음,이를 전제로 ① 이 사건 영장은 '피고인 2'를 피의자로 하여 '피고인 2가 공소외 1에게 지시하여 피고인 1을 통해 공천과 관련하여 ○○○당 공천심사위원인 공소외 13등에게 거액이 든 돈 봉투를 각 제공하였다'는 혐의사실을 범죄사실로 하여 발부된 것으로서 피고인 2의 정당후보자 관련 금품제공 혐의사건과 관련된 자료를 압수하라는 취지가 명백하므로,이 사건 영장에 기재된 범죄사실과 전혀 다른 '피고인 7과 피고인 1사이의 정당후보자 추천 및 선거운동 관련한 대가제공 요구 및 약속에 관한'혐의사실에는 그 효력이 미치지 아니하며,② 이 사건 녹음파일이 피고인 2에 대한 공소사실을 입증하는 간접증거로 사용될 수 있다는 것과 이 사건 녹음파일을 이 사건 영장 범죄사실과 무관한 피고인 7·피고인 1사이의 범죄사실을 입증하기 위한 증거로 사용하는 것은 별개의 문제이므로 피고인 2에 대한 관계에서 이 사건 녹음파일에 대한 압수가 적법하다고 하여 피고인 7,피고인 1에 대한 관계에서도 적법한 것은 아니라는 이유 등을 들어,검사가 별도의 압수

・수색영장을 발부받지 아니한 채 이 사건 녹음파일을 수집한 행위에는 적법하게 발부된 영장에 의하지 아니하고 증거를 수집한 절차적 위법이 있으므로,이에 따라 수집된 증거인 이 사건 녹음파일은 위법수집증거로서 그 증거능력이 없다고 판단하였다.

(나)기록에 의하면,이 사건 녹음파일에 의하여 그 범행이 의심되었던 혐의사실은 공직선거법상 정당후보자 추천 관련 내지 선거운동 관련 금품 요구・약속의 범행에 관한 것으로서,일응 범행의 객관적 내용만 볼 때에는 이 사건 영장에 기재된 범죄사실과 동종・유사의 범행에 해당한다고 볼 여지가 있다.그러나 이 사건 영장에서 당해 혐의사실을 범하였다고 의심된 '피의자'는 피고인 2에 한정되어 있는데,수사기관이 압수한 이 사건 녹음파일은 피고인 1과 피고인 7사이의 범행에 관한 것으로서 피고인 2가 그 범행에 가담 내지 관련되어 있다고 볼 만한 아무런 자료가 없다. 결국 이 사건 영장에 기재된 '피의자'인 피고인 2가 이 사건 녹음파일에 의하여 의심되는 혐의사실과 무관한 이상,수사기관이 별도의 압수・수색영장을 발부받지 아니한 채 압수된 이 사건 녹음파일은 형사소송법 제219조 에 의하여 수사기관의 압수에 준용되는 형사소송법(2011.7.18.법률 제10864호로 개정되어 2012.1.1.부터 시행된 것)제106조 제1항 이 규정하는 '피고사건'내지 같은 법 제215조 제1항 이 규정하는 '해당 사건'과 '관계가 있다고 인정할 수 있는 것'에 해당한다고 할 수 없으며,이와 같은 압수에는 헌법 제12조 제1항 후문,제3항 본문이 규정하는 헌법상 영장주의에 위반한 절차적 위법이 있다고 할 것이다.따라서

이 사건 녹음파일은 형사소송법 제308조의2 에서 정한 '적법한 절차에 따르지 아니하고 수집한 증거'로서 이를 증거로 쓸 수 없다고 할 것이고,그와 같은 절차적 위법은 헌법상 규정된 영장주의 내지 적법절차의 실질적 내용을 침해하는 중대한 위법에 해당하는 이상 예외적으로 그 증거능력을 인정할 수 있는 경우로 볼 수도 없다.

(다)그렇다면 수사기관의 이 사건 녹음파일 압수·수색 과정에서 피압수·수색 당사자인 피고인 1에게 참여권이 보장되었는지,복사대상 전자정보의 목록이 교부되었는지 여부 등은 별론으로 하더라도,원심이 위와 같은 전제에서 이 사건 녹음파일이 이 사건 영장에 의하여 압수할 수 있는 물건 내지 전자정보로 볼 수 없다고 하여 그 증거능력을 부정한 조치는 결론에 있어 정당한 것으로 수긍할 수 있으며, 거기에 검사의 상고이유 주장과 같이 범죄혐의 관련성의 범위나 위법수집증거배제법칙의 예외 등에 관한 법리를 오해한 위법이 없다.

4) 판례에 대한 언론 및 실무 동향

가) 언론

위 대법원 판결은 2013. 6. 5. 부산고등법원 2012노667 판결의 상고심이다. 부산고등법원 판결이 나온 후에 법률신문에서는 "왜 영장주의인가" 라는 취재수첩 기사를 작성하였다. 위 기사 내용은, 이 판결은 지난해 1월 시행된 개정 형사소송법이 영장으로 압수할 수

있는 증거물의 범위를 '압수수색 영장의 범죄사실과 관련 있는 것'으로 명확하게 규정한 이후 '관련성'의 구체적 범위를 처음으로 제시했다는 점에서 학계와 실무계로부터 큰 주목을 받고 있다. 하지만 검찰에서는 법원이 압수수색 영장의 범위를 지나치게 제한적으로 보고 수사범위를 축소해 수사를 번거롭게 한다는 볼멘 목소리가 나온다.[24]

나) 실무

위 사례에 대하여 오기두 부장판사는 관련성 원칙은 범죄혐의사실과 관련하여 주관적, 객관적, 시간적 관련성으로 세분화해 볼 수 있다. 주관적 관련성은 피의자로 특정한 사람에 한정하여 압수수색이 이루어져야 하는 것이고, 객관적 관련성은 압수수색 영장에 기재된 범죄혐의 사실과 관련된 증거에 한정, 시간적 관련성은 객관적인 범죄사실의 범행일시와 얼마나 관련되어 있는지에 따라 상대적으로 결정을 한다. 위와 같은 관련성 개념을 위 판결에 적용해 보면, 첫 번째 주관적 관련성 위반으로 이 사건 영장에 피의자는 최초 뇌물교부 혐의를 받던 甲으로만 기재되어 있는데, 당시 참고인 신분에 있는 乙의 휴대폰을 압수한 자체가 주관적 위반으로 보고 있다. 두 번째 객관적 관련성 위반으로 이 사건 두 공소사실은 기본적 사실관계마저 다른 완전히 별개의 범죄사실로 보고 있다. 그 논거로, 범죄일시가 1개월 정도 차이가 나고, 범죄 장소도 상이하다. 또한, 범행 주체도 다르기 때문에 객관적 관련성 위반으로 보고 있다.[25]

---

24) 신소영기자, "[취재수첩] 왜 영장주의인가", 법률신문2013. 6. 13. 법률신문 2013. 6. 13.자 https://www.lawtimes.co.kr/Legal-News/Legal-News-View?Serial=75759

25) 오기두, "관련성 없는 휴대폰 녹음 파일 압수와 위법수집증거", 법률신문 2013. 3. 4.자,

오기두 부장판사의 주장에 대하여 이완규 차장검사는 아래와 같은 사유로 반박을 하였다.[26]

> 이 사례에서 현재는 갑만 피의자로 입건되어 있으나 돈을 받은 을은 갑의 피의사실의 상대방이어서 갑과 을간의 통화나 그 내용을 담고 있을 을의 휴대폰은 갑의 피의사실의 증거로 관련성이 있으므로 당연히 압수수색의 대상이 된다. 그것이 갑 소유가 아니므로 압수할 수 없다는 식의 주장은 부적절하다.
> 한편, 현재는 갑만 피의자로 입건되어 있지만 향후 증거의 수집 상황에 따라 을도 공범으로서 또는 별건 피의자로서 수사대상이 될 것이 예견된다. 그리고 현재의 피의사실에 포함된 것은 갑으로부터 돈을 받은 행위뿐이지만 다른 사람으로부터 뇌물을 요구하는 범행은 을의 성행을 나타내는 것으로서 을에 대한 양형이나 갑의 진술에 대한 신빙성, 향후 을이 행할 진술의 신빙성을 판단할 수 있는 정황자료도 될 수 있으므로 현재의 피의사건과 관련성이 인정된다고 볼 것이다.
> 그러므로 이러한 경우 압수된 휴대폰 내에 녹음되어 있는 을과 K간의 대화부분은 현재 갑을 피의자로 하여 수사되고 있는 사건과 관련성이 있어 적법한 압수물이고, 그 압수물을 기초로 별건 범죄가 수사되는 경우 별도의 압수절차 없이(왜냐하면 현재의 사건에서 적법하게 압수되어 있으므로) 그 별건 범죄에 대한 증거로 사용할 수 있다고 할 것이다.

13면 참조

26) 이완규, "디지털 증거 압수수색과 관련성 개념의 해석", 법조 2013. 11월호, 70면

3. 우리나라 판례 관련성 개념 해석에 대한 평가

2009모1190 결정, 2011도10508 판결은 디지털 증거에 있어서 관련성 개념을 “혐의 사실과 관련된 부분으로 한정”하여 보았다. 혐의사실에 대하여는 2013도7101 판결에서 “형사소송법 제106조 제1항이 규정하는 ‘피고사건’ 내지 같은 법 제215조 제1항이 규정하는 ‘해당 사건’과 관계가 있다고 인정할 수 있는 것” 보고 있다. 즉, 그렇다면 관련성이 있다는 것은 압수수색 영장 청구 당시 범죄사실에 한정하는 것이다.

2009모1190 결정에서는 사건과 관련성이 없는 증거 수집에 대하여, “당사자 측의 참여하에 이루어진 위 압수·수색의 전 과정에 비추어 볼 때, 수사기관이 영장에 기재된 혐의사실의 일시로부터 소급하여 일정 시점 이후의 파일들만 복사한 것은 나름대로 혐의사실과 관련 있는 부분으로 대상을 제한하려고 노력을 한 것으로 보이고, 당사자측도 그 조치의 적합성에 대하여 묵시적으로 동의한 것으로 봄이 상당하므로, 결국 이 사건 범죄 혐의와 관련 있는 압수·수색의 대상을 보다 구체적으로 제한하기 위한 수사기관의 추가적인 조치가 없었다 하여 그 영장의 집행이 위법하다고 볼 수는 없다”고 판시하였다. 즉, 비록 관련성 없는 파일이 수집되었지만 당사자가 동의하였고 수사기관에서 나름대로 관련성 있는 파일을 압수하기 위해 노력한 점을 들어 영장 집행이 위법하다고 보지 않았다.

하지만, 2013도7101 판결에서는 사건과의 관련성을 엄격히 재단하여 최초 범죄사실로 압수한 휴대폰에서 취득한 증거를 이용하여 추가 범죄사실에 증거로 사용하는 것을 인정하지 않았다. 당시 피압수자는 참고인 신분이었고 장차 피의자 신분으로 예정이 되어 있었다.

위 참고인이 사용하는 휴대폰에는 첫 번째 범죄사실과 관련된 증거가 있었고, 추가로 위 참고인의 새로운 범죄사실과 관련되는 증거가 복원되었다. 하지만, 동 판결에서는 최초 범죄사실과 다른 범죄사실에 기 압수영장으로 확보한 증거를 사용할 수 없다고 보면서, 만약 위 증거를 다른 범죄사실의 증거로 사용하기 위해서는 추가로 압수수색영장을 판사한테 발부 받아야 한다고 판시하였다.

동판결 이후 수사기관에서는 위와 같은 사례가 발생하면 어떻게 대처를 해야 되는지에 대한 명확한 지침이나 지시사항이 없다. 기 압수한 증거물에서 새로운 범죄사실에 증거로 사용하기 위해서는 법원에 영장을 청구하게 되면, 대부분 법원에서는 별건 압수수색이라고 기각을 할 것임에는 자명한 사실이다. 후술하는 미국의 사례에서는 사건과 관련이 없는 다른 증거가 발견된 경우 원칙적으로 추가 압수수색 영장을 청구해야 한다고 보고 있다.

추가로 압수, 수색 영장을 청구한다고 하면 압수수색 대상물은 디지털 저장매체(휴대폰, 컴퓨터) 인지, 새롭게 발견된 해당 정보인지 우선 해결이 되어야 한다. 압수대상으로 정보가 해당되는지 여부에 대하여는 의견이 엇갈리고 있으며 이에 대한 세부적인 사항은 생략하기로 한다. 분명한 것은 법원에서 추가로 압수영장이 필요하다고 본 점은 압수 대상으로 디지털 저장 매체가 아니라 매체 안에 저장되어 있는 전자 정보를 말하는 것을 의미한다. 기 압수한 매체를 다시 압수수색 영장 청구하라는 것은 법리상 맞지 않는 것이고, 그렇다고 해도 전자 정보에 대하여 압수수색을 허용한 것이라고 하면 개정 형사소송법 제 106조 제3항에 규정한 '정보저장매체'가 압수수색 대상인 점과 맞지 않게 된다.

결국, 디지털 증거 관련하여 형사소송법 개정이 필요하며 압수 대

상으로 정보저장매체와 정보 2가지가 포함이 되어야 하고, 각각의 대상에 대한 압수수색 방법 또한 별도로 기술이 되어야 한다.

전자정보가 외국 입법례에서는 압수대상으로 포함이 되어 있는지에 대하여는 앞서 살펴본 이숙연 판사의 전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여 논문에서 다루고 있다.[27]

우리나라 법원은 미국의 사례를 많이 참고한 것으로 보이고, 미국은 연방 형사소송규칙에 압수할 물건(property)에 정보(information)를 포함하고 있다.[28] 아직, 국내 형사소송법은 압수 대상에 물건(정보저장매체)만 기재가 되어 있는 상황에서 법원에서는 추가로 압수수색 영장을 청구하라는 것은 법 개정이 되지 않은 상황에서 수사기관에게 법에 명시되지 않은 압수수색 영장을 요구하고 있는 것이다.

형사소송법이 다시 개정되기 위해서는 많은 시간이 걸리고, 압수대상에 정보를 포함시킬지 여부에 대하여 찬반 여러 의견이 있을 것이다. 법 개정 전까지는 법원과 수사기관이 조율하여 디지털 증거 관련하여 사건과 관련 없는 범죄에 대한 증거를 발견하게 되는 경우 압수수색 영장을 청구할 수 있도록 협의를 해야 한다. 협의가 되지 않은 상황에서 수사기관이 기 압수한 압수물에 대하여 재차 영장 청구를 하면 판사는 별건 압수수색이라고 기각할 것임을 명확하다.

물론 수사기관의 입장에서는 정당한 절차에 따라 확보한 증거물에 대하여 재차 법원에 영장 청구하는 것은 상당히 번거로운 일임

---

27) 이숙연, “전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여”, 헌법학연구 제18권 제1호, 2012. 3월호

28) 연방소송규칙 제 41조 압수수색, 정의를 보면 “Property includes documents, books, papers, any tangible objects, and information."

에 분명하다. 우리나라 범죄 발생 비율에 수사 인력이 부족한 실정이며, 새로운 압수수색 영장을 청구하기 위해서는 수사기관에서는 영장청구서를 작성하고 내부 결재 과정을 거쳐 법원에 청구를 하는데, 통상 법원에서는 검찰 압수수색 영장은 당직 판사가 결정하지 않고 다음 날 영장 전담 판사가 내용을 보고 발부 여부를 결정한다. 이런 기존 절차를 따르게 되면 추가 영장을 발부 받기 위해서는 2일이 소요가 된다.

신속하게 수사를 해야 하는 수사기관 입장에서는 2일이나 시간이 걸리는 것은 시간 낭비이고, 그 사이 증거가 변형이 될 수 있으며 여러 변수가 발생할 수 있다. 따라서 디지털 증거 관련 추가 압수수색영장은 새로운 영장 양식에 의거 기 압수한 영장을 토대로 새로운 증거가 발견되었고, 새로운 증거가 범죄사실과의 관련성에 대한 소명만 작성하여 청구를 하고, 영장 재청구의 취지에 따라 신속하게 법원에서 발부 여부가 결정이 되어야 한다.

4. 미국 실무 및 판례에 있어서 관련성 검토

가. 미국 실무

미국 연방 법무부 산하 연구기관인 'Office of Legal Education Executive Office for United States Attorneys'에서 2009년 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation'(범죄수사에 있어 디지털 증거 획득 및 압수수색 매뉴얼) 3번째 개정판을 발간하였다. 동 매뉴얼은 미국 수사기관을 위하여 디지털 증거 압수 및 분석을 위해 각종 법

규 및 판례의 예시를 들고 있다. 매뉴얼 90페이지 포렌식 분석 카테고리에 새로운 영장의 필요성에 대하여 설명하고 있다.

> 하나의 개인 컴퓨터는 여러 종류의 범죄에 연루될 수 있다. 그래서 컴퓨터 하드드라이브는 다수 다른 범죄의 증거들이 포함되어 있다. 수사관이 영장에 의해 컴퓨터를 수색할 경우, 보통 압수영장은 어떤 특정된 범죄에 대한 증거만 검색하는 것으로 한정하여 발부가 될 것이다. 이런 경우 수사관이 영장에 기재되지 않은 범죄에 대한 증거를 발견한 경우 새로운 영장을 발부 받아야 한다.[29]

즉, 범죄현장에서 범죄사실에 기재된 것과 다른 범죄에 사용된 증거가 발견되면 새로운 영장을 법원으로부터 발부 받으라는 안내이다. 이어서 지침에는 위와 관련된 법원의 판결례를 설명하면서 마약판매로 압수수색영장을 발부 받아 집행하는데, 피의자 컴퓨터에서 마약판매 관련 증거가 나오지 않은 상황에서 아동포르노물이 발견되었다. 그러자, 수사관은 마약판매 증거 관련하여 추가 수집은 포기하고 아동포르노물을 집중적으로 수색하였다. 이런 상황에서 연방 제10항소법원은 아동포르노물 증거를 배제하였고, 그 사유로 최초 영장 기재사항의 범죄사실의 범위를 초과하였다고 판단하였다.[30] 또 다른 예시로, 압수수색 현장에서 수사관이 첫 번째 범죄사실에 대한 증거를 수색하기 위해서 피의자 컴퓨터에 대하여 체계적인 검색을

29) A single computer can be involved in several types of crimes, so a computer hard drive might contain evidence of several different crimes. When an agent searches a computer under the authority of a warrant, however, the warrant will often authorize a search of the computer only for evidence of certain specified crimes. If the agent comes across evidence of a crime that is not identified by the warrant, it may be a safe practice to obtain a second warrant.

30) United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)

수행하는 과정 중에 일부 아동포로노물이 발견된 상황이라면, 추가적인 증거는 명인법리(plain view doctrine)[31]에 의거 압수수색할 수 있다고 보았다.[32]

동 지침에서는 결론으로 Carey 판결은 아직 배제가 된 것이 아니기 때문에 수사기관에서는 최초 영장에 기재되지 아니한 범죄사실에 대한 증거가 발견된 경우 신중하게 추가로 압수수색 영장을 발부 받아야 된다고 조언을 하고 있다.[33]

나. 미국 판례

1) 압수현장에서 증거 수색시 추가 증거 발견한 경우

압수현장에서 디지털 증거물을 탐색하는 것은 시간이 많이 소요되어 보통 미국 법원에서는 압수현장에서 디지털 기기를 압수하여 분석실시에서 추가 수색하는 2단계 구조를 인정하고 있다. 하지만, 수사기관에서 직접 컴퓨터를 수색하는 과정 중에 추가로 다른 범행

31) 손동권, "수사절차상 긴급 압수·수색 제도와 그에 관한 개선입법론", 경희대학교 법학연구소, <경희법학> 46권3호 (2011), pp.9-33에 명인법리에 관하여, "Plain View Doctrine'이란 수사기관이 적법하게 위치할 수 있는 장소에서 시야 내에 보이는 물건에 대해서는 그 물건이 범죄와 관련되어 있다고 믿을 만한 상당한 이유가 있어 압수의 대상임이 명백한 경우에는 영장 없이 긴급 압수할 수 있다는 것이다"라고 설명하고 있다.

32) Gray, 78 F. Supp. 2d at 531 n.11, "[a]rguably, [the agent] could have continued his systematic search of defendant's computer files pursuant to the first search warrant, and, as long as he was searching for the items listed in the warrant, any child pornography discovered in the course of that search could have been seized under the 'plain view' doctrine."

33) 이완규, "디지털 증거 압수수색 관련성 개념의 해석", 법조, 2013. 11월호, 하지만 본 논문은 Carey에서 제시한 주관적 기준은 독특한 것으로서 디지털 증거와 관련된 글들에서는 많이 언급되기는 하나 실제사건에서는 거의 따르지 않는다. 제10순회법원도 United States v. Burgess 사건에서 그 목적이 아니라 수색이 합리적인가에 중점을 둠으로써 Carey사건에서 행했던 주관적 기준의 실험은 종료되었다고 보고 있다.

의 증거가 발견되면 앞에서 살펴보았듯이 명인법리나 추가 영장이 필요한 것으로 보고 있다. 수사실무에서는 추가 영장으로 하는 것이 보다 더 안전한 장치라고 생각하고 있다.

2) 증거 원본 압수 후 분석하는 경우

수사기관에서 압수수색 영장을 청구할 때 청구서에 디지털 기기를 사본하거나 원본을 압수하여 분석실에서 추가 압수수색이 필요한 사유를 상세히 기술을 하게 되면, 대부분 미국 법원에서는 압수현장에서 디지털 기기를 압수 수색 하는 것은 시간이 많이 소요되고 오히려 피압수자에게 피해가 가는 것을 방지하기 위하여 2단계(two-step) 압수수색 절차를 허용하고 있다. 즉, 압수수색 현장에서 증거를 이미징하거나 원본을 압수한 후 디지털포렌식 분석실에서 증거물을 추가로 수색(탐색, search)을 하는 것이다.

이는 법원에서 디지털 기기의 특성상 관련성 없는 압수수색을 허용하고 있는 것으로 보인다. 하지만, 법원에서는 디지털 증거사본이나 증거원본을 압수하는 것은 허용하지만 추가로 분석 과정에 다른 증거가 발견된 경우 명인법리를 제외하고는 추가 영장 없이는 다른 범죄 사실에 증거로 사용할 수 없다고 보고 있다.

하지만, 최근 미국 법원에서는 위와 같은 2단계 압수수색 절차에 일정한 제약 조건을 두는 사례도 있고, 어떤 경우는 디지털 기기 원본 압수를 제한한 판결도 나오기 시작하고 있다.

법원에서 통상 이러한 절차를 허용하고 있기 때문에, 피고인측 변호인은 수사기관에서 압수한 디지털 증거물에 대하여 압수 범위를 초과하였다는 취지로 증거배제 신청을 한다. 피고인측은 증거배제

신청을 하는 근거로 수사기관에서 영장을 노골적으로 무시(Flagrant Disreguard)하여 영장 범위를 초과하여 디지털 증거를 압수하였다고 주장을 한다. 하지만, 대부분의 법원에서는 피고인의 증거배제 신청을 받아들여주지 않고 있다.

가) 허용 판례

(1) Hill, 459 F.3d 966, 974-75(9th Cir. 2006)

(가) 사건개요

컴퓨터 기술자가 피고인의 컴퓨터를 수리하다가 아동포로노물이 저장되어 있는 것을 발견하였다. 즉시, 위 기술자는 경찰에 신고하였고 해당 경찰은 법원에 압수수색영장을 청구하였다. 해당 압수수색 영장은 컴퓨터 수리점을 수색하고 "[a]ll storage media belonging to either [the computer] or the individual identifying himself as [defendant] at the location," and "[a]ll sexually explicit images depicting minor[s] contained in [the storage media]." 와 관련된 해당 컴퓨터, 컴퓨터와 관련된 작업지시서가 포함되었다. 경찰이 컴퓨터 수리점에 압수수색영장을 집행하러 갔을 때 피고인은 해당 컴퓨터를 가지고 가고 있었다. 그래서, 경찰은 압수수색영장에 따라 피고인 컴퓨터를 압수수색하였다. 이어서 경찰은 피고인의 주거지와 컴퓨터 등에 대한 추가 압수수색 영장을 신청하였다.

경찰이 피고인의 주거지에 대하여 압수수색영장을 집행하였는데 추가로 컴퓨터가 없었지만, 피고인의 침실로 추정되는 방에서 외부

저장매체(집드라이브)를 발견하여 압수하였다. 결국 나중에 해당 외부저장매체에서 아동포르노물이 발견되어 피고인은 기소되었다.

(나) 피고인 주장

첫 번째, 피고인은 압수수색영장에 첨부된 선서진술서에는 자신이 아동포로노물을 가지고 있었다는 것에 대한 상당성(probable cause)이 없었다고 주장. 두 번째, 압수수색영장은 너무 광범위했다고 주장하면서, 압수수색영장은 해당기기에 아동포로노물이 저장여부에 상관없이 모두 압수수색을 허용하였고, 압수영장은 해당기기를 압수 후 포렌식 조사에 일정한 제한을 두지 않았다고 주장하였다.

(다) 법원 판단

해당 압수수색영장에는 압수집행시 컴퓨터 수집 장치 혹은 포렌식 전문가가 요구되지 않았다. 설령 위와 같은 장비, 전문가가 있었다고 하더라도 압수수색 현장에서 컴퓨터를 조작하거나 증거 수집시 진정성이 훼손될 수 있다. 이러한 이유로 디지털 기기를 사본 후 분석을 해야 한다. 그리고, 압수수색현장에서 파일 검색하는 것은 상당히 시간이 오래 소요된다. 이렇게 시간이 많이 걸리는 것은 수사자원에 상당히 부담이 되고 수색에 도움이 되지 않는다. 또한, 수사기관이 압수수색 현장을 통제하기 때문에 그 시간만큼 피압수자한테 피해가 간다. 그렇기 때문에 수정헌법의 가치를 절충하여 압수수색현장은 가능한 간단하고 덜 침해가 가는 방향으로 해야 한다고 판단하였다.

(2) United States v. Joseph Schesso (9th Cir. 2013)

(가) 사건개요

2008년 가을경 독일수사기관은 eDonkey라는 p2p(peer-to-peer)[34] 파일공유네트워크를 통하여 아동 포르노물이 배포 되는 사건을 수사하고 있었다. 수사기관에서는 2008년 10월경 4시간동안 18분 가량 되는 아동포르노물이 미국에 위치한 특정 IP에서 다운로드가 가능하게 해 놓은 것을 발견하였다. 독일수사기관은 미국 ICE(미국이민세관집행국)에 공조수사 요청을 하였고, 위 ICE 특별수사관 Julie Peay는 위 IP 주소는 워싱턴주 밴쿠버에 있는 Schesso에 할당된 것을 확인했다.

수사기관에서의 선서진술서 내용을 보면, 컴퓨터의 저장 용량, 아동포르노물을 인터넷 p2p을 통해 배포한점, 아동포르노물 수집자들의 알려진 성향에 따르면 은닉할 가능성이 농후한점에 대하여 설명하였다. 선서진술서는 더 나아가서 디지털증거의 저장용량이 크고 관련된 디지털 증거를 찾기 위해서는 전문적인 장비와 전문가가 필요해서, 해당 디지털 증거를 주거지에서 압수한 후 통제된 디지털분석실에서 추가 분석을 해야 할 필요성에 대하여 기술하였다.

영장에는 압수수색 제한이나 관련성 없는 증거 환부에 대해서는 언급을 하지 않았다. 이민국과 밴쿠버 경찰이 합동으로 피고인 주거지에 대한 압수수색을 실시하였고, 피고인은 자신이 p2p 프로그램을

34) P2P는 네트워크를 통해 연결되어 있는 모든 개인용 컴퓨터가 서버와 클라이언트 기능을 하는 네트워크 시스템이다. 서로 네트워크로 연결되어 있는 컴퓨터 상호간에는 다양한 자료(불법, 적법 모두 포함)를 서로 주고 받을 수 있다. P2P를 최초 소개한 것은 1999년 숀 패닝(Sha주 Fanning)이 냅스터를 통해 소개하였다.

이용하여 지난 몇 년간 아동포르노물 다운로드 받아 보았다고 인터뷰에서 진술하였다. 수사기관은 피고인 주거지에서 데스크탑 PC와 카메라 메모리 카드를 포함하여 다양한 디지털 기기를 압수하였다. 압수한 디지털 증거에 대하여는 포렌식 전문가가 분석을 하였고, 피고인이 말한 음란물 보다 상회하는 3,400개 이미지와 632개의 사진 아동포르노물을 발견하였다. 또한, 카메라 메모리카드에서 피고인의 약혼녀의 삭제된 음란 사진 또한 복구하였다.

검찰에서는 피고인을 기소하였고, 피고인은 자신의 주거지에서 압수한 모든 증거에 대하여 증거배제 신청을 하였다. 피고인은 증거배제 신청의 근거로 CDT Ⅲ(미국 제9항소법원에서 압수수색 방법제한)에 따라 압수수색 방법 제한(protocol)에 따른 절차 안전장치가 없었다고 주장하였다. 주 법원에서는 피고인의 증거배제 신청을 받아들였다.

(나) 항소법원 판단

항소법원에서는 모든 주어진 상황을 보았을 때 피고인의 컴퓨터와 다른 저장매체에 아동포르노물이 있을 가능성이 있었고, 이를 근거로 압수영장이 발부된 것은 실제적이고 상식적인 결정이라면서 주 법원의 증거배제 신청이 잘못되었다고 지적하였다.

이어서, 항소법원에서는 수사기관에서 디지털 증거 수색하는 어려움을 이해하면서, 수사기관에서는 어느 디지털 기기에서 얼마나 많은 불법적인 파일이 있을지 혹은 어디에 저장되어 있는지를 알 수 없으며, 또한 압수 대상물을 정확히 기술할 방법이 없다. 이런 사실로, 본건 영장은 압수현장 이외에서 분석과 복구의 필요성을 상세히

기술하였고, 수사기관이 현장에서의 피고인 증거 압수와 포렌식 분석실에서의 2단계 압수수색은 정당하다고 판결하였다.[35]

(3) United States v. Ganias, 755. F.3d 125(2nd Cir. 2014)

압수수색 현장에서 디지털 증거를 수색하는 것은 개인뿐만 아니라 정부에도 큰 부담이 된다. 그래서 디지털 증거는 사본을 하여 추후 분석을 하는 것이 대부분의 사례에서 헌법위반으로 보고 있지 않다.[36] 물론 일반 물건에 대한 위와 같은 압수수색은 허용하지 않는다.

2009년 형사소송절차가 개정되어 어떤 특정한 상황에서는 압수수색 이외의 현장에서 수색을 허용하게 되었다. 비록 피고인의 사건은 2003년 발생한 것이지만 수사기관은 정당한 절차에 의해 압수수색을 하였고, 당시 판례법에서도 위와 같은 압수 현장 이외에서의 수색은 필요하고 합리적이라고 보았다.

하지만, 디지털 증거 사본을 이용하여 압수현장 이외에서의 분석은 여전히 합리성을 따라야 한다. 2009년 형사소송절차 자문위원회의 문서를 보면 합리성이 어떤 개념인지 알 수 있다. 특히 위원회는 압수수색 이후 증거사본을 언제까지 해야 되는지, 그리고 해당 증거

35) 미국 연방형사소송절차 41(e)(2)(b)를 보면 원본 압수와 해당 기기 사본(이미징)을 하여 압수 현장 이외에서 탐색할 수 있다. Lacy, 119 F.3d at 746 (9th Cir.1997)를 판결을 보면, 수사기관이 2개의 불법적인 아동 포르노 사진이 어디에 저장되어 있는지 확인할 수 없어 컴퓨터 전체를 압수하는 포괄적인 압수가 필요하다고 보았다.

36) 미국 대부분 법원에서 디지털 기기 매체 특성상 압수수색 현장에서 모든 디지털 증거를 분석하고 수색하는 것이 불가능하고, 이런 수색 행위가 정부 인력 낭비뿐만 아니라 압수를 당하는 피압수자에도 크나큰 피해가 초래하기 때문에 대부분 2단계 압수수색을 허용하고 있다.

사본을 분석하는 것에 대한 종기를 두는 것에 대하여 반대하였다. 이에 대한 자료로 자문위원회는 디지털 기기의 저장 용량, 암호문서 혹은 증거 함정 그리고 컴퓨터 포렌식 분석실 부하의 요소를 거론하면서 모든 사건에 획일적인 증거분석 기간을 정하는 것에 대하여 반대하였다. 이러한, 사실들은 압수수색 현장이외에서의 추가 분석에 대하여 정당성을 부여한 것이다. 하지만, 그렇다고 해도 영장 범죄사실 이외의 추가적인 범죄사실에 대한 증거를 확보하는 것에 대한 독립적인 근거를 마련한 것은 아니라고 보았다.[37]

나) 부정 판례

(1) Riley v. California, 134 S.Ct. 2473 (2014. 6. 25.)

위 미국 대법원 판결은 2명의 피고인에 대한 사례로 체포 현장에서 영장 없이 피고인의 휴대폰에 대한 압수수색하여 증거를 확보한 것에 대하여 법원이 증거배제 결정을 한 사례이다. 동 대법원 판결은 국내외적으로 기념비적인 판결로 평가되고 있으며, 디지털 증거

37) The advisory committee's notes to the 2009 amendment of the Federal Rules of Criminal Procedure shed some light on what is "reasonable" in this context. Specifically, the committee rejected "a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place." Fed.R.Crim.P. 41(e)(2)(B) advisory committee's notes to the 2009 Amendments. The committee noted that several variables—storage capacity of media, difficulties created by encryption or electronic booby traps, and computer-lab workload—influence the duration of a forensic analysis and counsel against a "one size fits all" time period. Id. In combination, these factors might justify an off-site review lasting for a significant period of time. They do not, however, provide an "independent basis" for retaining any electronic data "other than [those] specified in the warrant." United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1171 (9th Cir.2010) (en banc).

관련 대법원에서 판결한 몇 개 안되는 판결 중 하나이다. 추후 미국 하급심에서는 동 판결 취지를 바탕으로 디지털 증거 압수수색의 허용여부 및 적법성에 대하여 판단할 것으로 보인다. 이에, 본 논문에서는 대법원 판결의 주요 내용에 대하여 원문 그대로 번역하여 자세한 내용을 살펴보도록 하겠다.

(가) 사건개요

첫 번째 피고인은 David Riley이고, 위 피고인은 자동차등록번호 등록기간이 만료된 것으로 경찰의 불심검문에 단속이 되었다. 또한 불심검문중에 경찰관은 피고인의 운전면허가 정지된 것을 발견하였다. 경찰관은 피고인의 차량을 압수하였고 또 다른 경찰관은 차량을 수색하는 도중에 차량 후드 아래 은닉된 총기를 발견하였고 피고인을 총기 소지 혐의로 체포하였다. 경찰관은 피고인을 체포하는 과정중에 피고인의 바지 주머니에서 스마트폰을 압수하고, 휴대폰을 검색하는 도중 갱단 멤버들이 사용하는 은어로 알 수 있는 문자메세지와 연락처를 확보하였다.

피고인은 체포된 이후 2시간이 지나서 조직폭력 전담 수사관이 피고인의 휴대폰에서 피고인이 갱단에 관여가 된 동영상 일부를 발견하였고, 추가로 지난 몇 주 전에 발생한 차량 총기 사건과 관련된 차량 앞에서 피고인이 서 있는 사진을 발견하였다. 수사기관은 피고인을 몇 주 전에 발생한 차량 총기 사건, 주차된 차량에 방화한 사건, 총기로 폭행한 사건, 그리고 살인미수 혐의로 기소하였다.

피고인은 영장 없이 자신의 휴대폰을 압수수색한 것은 수정헌법을 위반한 것이라고 증거배제신청을 했으나 기각 당하였고, 피고인

은 위 혐의로 징역 15년을 선고 받았다. 피고인은 항소하였지만, 항소법원 역시 피고인의 휴대폰에서 발견한 증거에 대하여 배제신청을 받아들여 주지 않았다.

두 번째 피고인은 Brima Wurie이고, 위 피고인은 차량에서 마약 판매 혐의로 경찰에 적발이 되었다. 경찰관은 피고인을 체포하여 경찰서로 연행하였고, 피고인이 소지하고 있던 휴대폰 2개(피쳐폰, 스마트폰)를 압수하였다. 경찰서에 도착하기 약 10분전에 경찰관은 피고인의 피쳐폰 외부 화면에서 'my house' 라는 연락처에서 계속적으로 전화가 온 것을 확인했다. 몇 분 지나서 경찰관은 위 휴대폰 플립을 열어보았고, 여자와 아기가 있는 배경화면이 있었고, 버튼을 눌러 통화기록을 확인하였고 위 'my house' 전화번호를 찾았다. 경찰관은 위 전화번호를 인터넷 전화기록부에서 검색하여 어느 아파트에 할당이 된 것을 발견하였다. 그래서 경찰관이 아파트에 가보았고, 피고인의 우편함이 있었고 조금 전에 보았던 휴대폰 배경화면에 있었던 여자가 아파트에 있었다. 경찰관은 현장을 보존하였고 법원에서 압수영장을 발부받아 아파트에서 215그램 코카인 등을 압수하였다. 피고인은 코카인 배급 및 코카인을 배급하기 위해 보관, 그리고 총기와 탄약을 보관한 혐의로 기소되었다.

피고인 역시 휴대폰으로부터 얻은 정보를 토대로 피고인의 아파트에서 압수한 것은 독수과실에 따른 것이라면서 증거배제 신청을 하였지만 기각당하였고 262개월 징역형을 선고 받았다.

(나) 체포현장에서 휴대폰 압수에 관하여

체포현장에서 압수의 필요성은 체포하는 사람의 안전과 증거 보

전의 필요성을 충족해야 한다. 일반 물건에 대한 압수는 위와 같은 원칙에 따라 이루어지면 되지만, 본 사건의 휴대폰[38] 역시 같은 논리로 증거 보전의 필요성에 의해 압수가 가능한지 살펴보았다. 판결에서는 개인의 프라이버시 보호와 법집행기관의 필요성에 대한 이익형량으로 비교하였다. 전통적인 물적 증거를 체포 당시 피의자로부터 압수하는 것과, 단순히 휴대폰을 압수하는 것을 비교할 수 있는지 의문점을 들면서, 휴대폰은 문자 그대로 방대한 개인정보가 저장되어 있기 때문에, 일반 물건을 압수 하는 것과 휴대폰을 압수 하는 것은 비교 자체가 되지 않는다고 보았다. 따라서, 수사기관에서는 대신 압수수색영장을 청구하여 휴대폰에 대한 수색을 해야 한다고 판단하였다.

(다) 수정헌법의 의의[39]

수정헌법의 궁극적인 기준은 합리성(reasonableness)으로, 합리성을 바탕으로 본건 케이스를 살펴보았다.

휴대폰에 저장되어 있는 디지털 증거는 그 자체로 체포하는 경찰관에게 무기로 사용되어 위협적인 상황이 발생하지 않는다. 예를 들어, 경찰관이 현행범인을 체포하는 과정에 소지품 중 담뱃값을 발견한 경우, 경찰관이 담뱃값을 압수하면 범인은 이후 담뱃값의 내용물을 확인할 수 없다. 하지만, 위와 같은 사례에서 체포하는 현장의

38) 본 판결에서 대법관은 휴대폰에 대하여 “such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy”라고 보았다.

39) The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

분위기나 미묘한 분위기상 담뱃값 안에 담배가 들어 있지 않고 다른 물건이 들어 있을 수 있다. 이러한 경우 실제 담뱃값 안에 어떤 물건(무기 등)이 있는지 추가로 수색하는 것은 합리적이라 볼 수 있다. 하지만, 디지털 기기에서는 이런 불확실성을 상정할 수 없다.

물론 수사기관에서는 체포자가 휴대폰으로 공범자와 연락을 취하여 현장에 올 수 있게 하면 간접적으로 체포하는 경찰관에게 위협적인 요소가 될 수 있다고 주장할 수 있다. 하지만, 미국법은 현장의 실제 경험을 바탕으로 해서 만들어진 것이 아니기 때문에, 이런 주장은 각 케이스마다 다를 수 있으며 케이스별로 분석을 해야 한다.

(라) 증거 손상 방지 차원에서 휴대폰 압수한 것에 대한 판단

경찰관이 현행범인의 휴대폰을 물리적으로 압수하게 되면 해당 범인이 추가적으로 휴대폰에 물리적인 손상을 가할 위험은 거의 없다.

이에 대하여, 수가기관에서는 휴대폰에 저장되어 있는 자료는 원격 자료 삭제[40], 데이터 암호와 같은 것에 있어 상당히 취약하다고

40) Zack Whittaker, "Smartphones 'remotely wiped' in police custody, as encryption vs. law enforcement heats up", http://www.zdnet.com/article/smartphones-remotely-wiped-in-police-custody-as-encryption-vs-law-enforcement-heats-up/
영국 경찰은 지난 몇 년 동안 자신들이 압수한 모바일 폰 6개가 원격 삭제 되어되어 현재 진행중인 사건에서 중요한 증거가 인멸되었다. 이러한 원격 삭제는 휴대폰 분실에 대비하여 제조사가 만든 기술로, 최근 스마트폰인 애플 아이폰, 안드로이드 및 윈도우폰 운영체제 대부분 탑재하고 있다.
영국 포렌식 전문가에 따르면, 만약 휴대폰이 신호를 받을 수 있는 상태이면 원격삭제가 이론상 가능하다고 보고 있다. 물론 수사기관에서는 전자파 차폐 봉투에 스마트폰을 압수하지만, 어떤 사례에서는 스마트폰을 압수하는 짧은 과정 중 즉, 스마트폰이 위 봉투에 넣기 전의 순간에 외부에서 원격 신호가 들어 올 수 있으며, 위 신호에 따라 휴대폰에 들어 있는 모든 데이터가 삭제가 된다.

주장하고 있다. 원격삭제는 휴대폰이 통신 가능 상태에 있으면 원격 삭제 신호를 받고 이루어진다. 이는 제 3자가 원격 신호를 보내거나 휴대폰이 어떤 특정한 위치에 있게 되면 미리 자동화프로그램에 따라 데이터가 원격 삭제가 이루어진다. 암호화는 패스워드로 휴대폰을 보호하는 것을 넘어 휴대폰의 내용을 암호화 하는 것이다. 휴대폰이 잠겨져 있어 패스워드를 모르면 휴대폰에 저장되어 있는 데이터는 암호화 되어 있기 때문에 그 내용을 확인할 수 없다.

이런 휴대폰의 증거 손상의 광범위한 사례는 당연히 물리적인 증거에 있어서의 손상과 구별된다. 원격삭제는 체포현장에 없는 원격지에 있는 제 3자이고, 휴대폰 암호화는 물론 더 멀리 떨어져있다. 이러한 주장은 체포현장에서 발생하는 증거 손상이나 은닉과 거리가 멀다.

법원에서는 이런 사례가 극히 드물다고 보고 있다. 체포자에 의한 원격삭제 사례는 일화적인 것이고, 암호화 사례 역시 경찰관이 현행범인 체포할 때 휴대폰이 잠겨져 있는 것을 발견하는 것이 극히 이례적이다. 왜냐하면, 대부분 휴대폰은 버튼에 의해 잠겨지거나 초기 설정이 대부분 비활성화 시간이 얼마 지나면 잠겨지게 되어 있다(아이폰 iOS 7.1 유저가이드를 보면 1분으로 설정되어 있음).[41]

최근 미국 수사기관에서는 구글과 애플에 스마트폰의 초기 설정이 암호화 하는 것에 대하여 항의를 하였다. FBI, NSA 수사기관에서는 이러한 제조사들의 암호 설정으로 수사에 난항을 겪고 있다고 전하고 있다. 데이터 암호 설정으로 마약 밀매 거래, 범인 식별이 힘들어 지고 있다.

이어서, 영국 수사기관은 이런 암호화에 대비하여 만약에 범인이 패스워드를 말하지 않으면, 추가로 최고 징역 2년 범위에서 형을 추가하는 방향을 모색하고 있다. 하지만, 미국 같은 경우 수정헌법에 의거 자기부죄에 의해 보호되기 때문에 적용이 될 수 없다고 보고 있다.

또한, 원격삭제 같은 경우도 암호화와 마찬가지로 중요한 데이터에 대하여 원격삭제를 하면 추가로 형량을 늘리는 것을 고려해 볼 수 있다.

41) 김익현 기자, “아이폰, 얼굴만 갖다대면 바로 잠금 해제?”, ZDNET KOREA, 2015. 4. 1. 애플이 얼굴인식 기술을 활용해 모바일 기기 잠금을 해제하는 특허권을 취득했다고 리

휴대폰 데이터 원격삭제는 수사기관에서 위협에 대처할 만한 구체적인 방법이 아예 없지는 않다. 휴대폰을 압수하고 나서 즉시 데이터를 차단(비행기 모드, 차폐 봉투)하게 되면 원격삭제가 이루어질 수 없다. 휴대폰 전원을 끄고 배터리를 분리하거나, 휴대폰이 암호화 되어 있으며 전자파 차폐 봉투(Faraday bags)에 넣으면 된다.

수사기관에서는 현행범인을 체포하는 과정 중에 휴대폰을 발견하게 되면 이러한 조치를 취한 후에 법원에 추가 압수수색 영장을 청구하고 대기해야 한다.

(마) 휴대폰 압수는 일반 물건 압수와 별반 차이가 없다는 주장에 대한 판단

수사기관에서는 체포현장에서 압수수색영장 없이 휴대폰에 저장되어 있는 자료를 압수수색하는 것은 범인이 소지하고 있는 물건에 대한 압수수색과 별반 차이가 없다고 주장하고 있다. 하지만, 이는 극명하게 차이가 나는 것이고 예를 들어 말을 타는 것과 우주선을 타고 달에 가는 것과의 차이만큼 간극이 있는 것이다. 물론 두 가지

코드가 31일(현지 시각) 보도했다. 이번에 애플이 취득한 특허권은 스마트폰의 카메라가 이용자의 얼굴 이미지를 분석한 뒤 등록된 소유자와 일치할 경우 잠금을 해제해주는 기능이다.

이 기능을 도입할 경우 모바일 기기 잠금 상태를 해제할 때 불필요하게 소요되는 시간을 줄일 수 있을 것이라고 애플이 설명했다. 일반적으로 스마트폰을 이용할 때는 얼굴 가까이 들고 있는 경우가 많기 때문에 사실상 자동으로 잠금 해제가 될 수도 있다는 것. 따라서 패스워드가 필요 없게 된다는 것이 애플의 설명이다.

앞으로 기술의 비약적인 발달로, 수사기관의 디지털 증거 확보는 점점 어려워 지고 있는 상황을 보여주고 있다. 애플 같은 경우 모든 데이터가 암호화되어 있기 때문에 이러한 보안 기술이 도입이 되면, 수사기관에서는 피의자의 스마트폰을 압수하여도 해당 내용을 볼 수 없는 사태에 이르게 될 것이다.

http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150401081022

모두 한 지점에서 다른 지점까지 이동하는 것은 같지만, 이를 같이 취급하는 것은 정당화될 수 없다. 현행범인이 소지하고 있는 물건을 수색하는 것은 더 이상 범인의 프라이버시를 추가로 침해하지 않지만 휴대폰을 포함하여 디지털 저장 매체에 대하여 수색하는 것은 하늘과 땅 차이만큼 크고, 범인의 프라이버시에 대하여 추가적인 침해가 크게 발생한다.

현행범인이 소지하고 있는 물건 중에 휴대폰과 다른 소지품과는 양적으로나 질적으로나 크나큰 차이가 있다. 휴대폰(cell phone)은 그 자체로 약칭으로 오도되지만, 휴대폰은 마이크로컴퓨터[42]가 탑재된 것이고 전화하는 것은 부수적인 것이다. 휴대폰(특히 스마트폰)은 카메라, 비디오 플레이어, rolodexes(미국 Zephyr American사의 회전 인출식 인덱스 파일의 상품명; 링에 철해진 카드가 회전해서 해

42) 휴대폰은 피쳐폰과 스마트폰을 포함한 개념이다. 그렇다면 피쳐폰과 스마트폰의 차이점은 운영체제가 설치되어 컴퓨터와 마찬가지로 다양한 연산을 할 수 있는지 여부에 따라 판명이 난다. 아래기사를 보면 스마트폰에 대하여 쉽게 개념 설명을 하고 있다.
이상우 기자, "컴퓨터와 휴대전화의 만남 스마트폰", IT동아
스마트폰 등장 이후 휴대전화 하나로 많은 것을 할 수 있는 세상이 왔다. 전화나 문자 메시지는 물론, 웹 서핑, 게임, 동영상 감상, 문서 열람 및 작성 등 여가를 즐기고 업무를 수행하는 데 있어 중요한 기기가 됐다. 미래창조과학부가 발표한 통계자료에 따르면 2015년 2월 국내 이동전화 가입자 수는 약 5,717만 명이며, 이 중 약 4,106만 명이 스마트폰을 사용한다. 국내 경제활동인구 대부분이 사용하는 셈이다.
컴퓨터가 작동하기 위해서는 운영체제(OS, Operation System)가 필요하다. 이는 스마트폰역시 마찬가지다. 컴퓨터용 운영체제가 윈도, OS X, 유닉스, 리눅스 등으로 다양한 것처럼 스마트폰도 다양한 운영체제가 있다. 오늘날 널리 쓰이는 운영체제는 구글 안드로이드와 애플 iOS다. 2014년 3분기를 기준으로 전세계 스마트폰 시장에서 운영체제별 점유율은 안드로이드 83.1%, iOS 12.7% 등이며, 이밖에 윈도 폰 3%, 블랙베리 0.4% 등이 뒤를 잇는다.
스마트폰의 핵심은 '애플리케이션(Application, 이하 앱)'이다. 앱(App)이란 응용 프로그램을 말한다. 우리가 윈도 PC에서 MS 워드, 인터넷 익스플로러 등을 사용하는 것처럼 스마트폰에서도 각 운영체제에 맞는 응용프로그램을 사용한다. 특히 스마트폰에 장착된 센서나 부품을 앱 구동에 활용할 수 있기 때문에, 가능성이 무궁무진하다. 카메라로 문서를 촬영하면 이를 텍스트로 바꿔주는 OCR 앱이나, 내장 GPS를 이용해 길을 안내해주는 지도 앱 등이 대표적인 사례다. 이뿐만 아니라 수평 센서, 가속도 센서, 전자 나침반 등의 내장센서를 이용하는 앱도 꾸준히 등장하고 있다.
http://navercast.naver.com/contents.nhn?rid=122&contents_id=4128

당부분을 자동적으로 검색할 수 있도록 되어있다), 달력, 테이프 레코더, 도서관, 다이어리, 앨범, 텔레비전, 지도, 신문을 볼 수 있다. 최근 휴대폰의 가장 큰 구별되는 특징은 극명하게 큰 저장용량을 들 수 있다. 휴대폰 이전에는 범인에 대한 수색은 프라이버시에 대한 적은 침해를 주었다. 대부분의 사람들은 지난 수개월 기간 동안 주고받은 이메일, 사진, 읽은 책이나 기사를 출력하여 소지하고 다닐 수 없으며, 또한 그렇게 시도할 이유가 없다. 설령 범인이 위와 같이 모든 것을 출력하여 트렁크에 소지하고 다닌다고 해도, 위 트렁크 내용물을 확인하기 위해서는 추가 압수수색 영장이 필요하다.

하지만, 휴대폰의 사례를 보면 개인프라이버시에 대한 침해는 물리적으로 한정되어 있지 않다. 최근 많이 팔리고 있는 스마트폰을 보면 16GB용량(64GB까지 확장 가능)을 가지고 있다[43]. 16GB 용량은 텍스트로 수백만 페이지이고, 수 천 장의 사진, 수 백 개의 동영상을 저장할 수 있다. 휴대폰은 다양한 종류의 정보를 저장할 수 있는 능력이 있다. 20달러 이하에 팔리는 보급형 휴대폰에도 카메라, 사진 메시지, 문자메세지, 인터넷 접속기록, 달력, 수천 개의 전화번호부, 기타 등등을 할 수 있다.

(바) 휴대폰은 개인 프라이버시의 총합체

43) 스마트폰 기본 내장메모리가 16~64GB이고, 추가로 마이크로SD 외장메모리를 장착하면 그 용량은 더욱 늘어난다. 2015. 5. 1. 에누리 상품비교사이트에서 마이크로SD를 검색해 본바, 삼성전자 microSDHC Class10 EVO UHS-1 32GB가 판매 1순위로 최저가는 10,810원이고, 2순위는 같은 제조사 128GB로 최저가는 86,800원임. 즉, 만원만 추가하면 휴대폰에 32GB 용량만큼 메모리가 추가되어 사진, 동영상 등을 추가로 더 저장할 수 있게 되었음. 그리고, 9만원을 추가하면 128GB라는 어마어마한 메모리 용량을 추가할 수 있게 되었다.

휴대폰의 저장용량은 개인 프라이버시와 상호 관련된 결과를 가지고 있다. 첫 번째, 하나의 휴대폰은 저장장소에 다양한 종류(주소, 메모, 처방전, 은행 입출금내역서, 동영상)의 정보를 저장하고 있다. 두 번째, 하나의 휴대폰은 이전의 다른 어떠한 기기보다 정보를 훨씬 더 잘 전송할 수 있다. 휴대폰에 저장되어 있는 날짜, 위치, 설명에 대한 정보가 있는 수천 장의 사진을 통하여 개인 사생활이 낱낱이 드러나고 재조합될 수 있다.[44] 이는 개인이 소지하고 있는 지갑에 들어 있는 사진을 압수하는 것으로는 알 수가 없는 정보이다. 세 번째, 휴대폰에 있는 정보는 휴대폰을 구입할 당시까지 거슬러 올라갈 수 있으며 혹은 심지어 더 이전까지 갈 수 있다. 마지막으로 휴대폰 자체로 특징이 있는 것이지 해당 물리적 기록에 대한 특징이 아니라는 만연한 요소가 있다.

디지털 시대 이전 사람들은 일상생활을 영위할 때 자신한테 민감한 정보를 소지하지 않고 다녔다. 현재는 온갖 개인정보가 들어있는 휴대폰을 소지하고 있지 않은 사람이 없을 정도이다. 여론조사에 다르면 심지어는 샤워중에도 휴대폰을 가지고 있다고 응답한 사람이 12% 되는 것으로 조사가 되었다.(mobile consumer habits study,

---

44) 이상우 기자, “이건 어디서 찍은 사진? 사진 속 위치정보 분석”, 2014. 10. 8., IT 동아,
스마트폰이 대중화되면서 익숙해진 정보도 있다. 바로 위치정보다. 스마트폰에 있는 GPS를 통해 사진을 찍은 위치까지(위도/경도 등) 넣을 수 있다. 여행을 좋아하는 사람에게는 이 위치정보가 아주 유용할 수 있다. 여행 중 사진을 찍은 것만으로 자신이 지나온 경로를 확인할 수 있는 것은 물론, 집에 돌아와 여행의 추억을 되새길 수도 있다. 하지만 일상적인 사진에서 위치정보는 조금 위험한 정보일 수 있다. 위치정보를 담아서 공유했다가는 자칫 ’신상’ 정보를 유출할 수 있기 때문이다.
그렇다면 사진에 담긴 위치정보는 어떻게 확인할 수 있을까? 가장 쉽게 확인하는 방법은 파일을 마우스 오른쪽 버튼으로 누른 뒤, 속성 > 자세히 > GPS 항목에서 해당 정보를 보면 된다. 여기서 보이는 정보는 위도와 경도다. 이 좌표를 구글 지도 등의 애플리케이션이나 위도/경도 확인 사이트 등에 입력하면 위치를 지도에서 확인할 수 있다. 만약 구글 지도를 이용한다면 37°30’24.7", 126°53’22.1" 같은 방식으로 위도와 경도를 함께 입력하면(쉼표로 구분) 된다.
http://it.donga.com/19427/

june 2013).[45] 십년 전에는 경찰관은 현행범으로부터 개인적인 정보가 들어 있는 다이어리 같은 것을 우연히 발견할 수 있었다. 그러나, 이러한 다이어리를 발견한 사례는 거의 드물었다. 반대로 오늘날 미국 성인의 90% 이상은 자신의 중요하거나 시시콜콜한 정보가 저장되어 있는 휴대폰을 가지고 다닌다는 것은 결코 과장된 표현이 아니다. 경찰관에게 그러한 정보가 들어 있는 휴대폰을 수색하라고 건네주는 것은 자신의 개인적인 물건 몇 개를 주는 것과 비교를 할 수 없다.

비록 휴대폰에 저장되어 있는 정보는 물리적 기록과 양적으로 구분이 된다. 또한 어떤 정보는 질적으로도 차이가 있다. 예를 들어, 인터넷 검색과 히스토리 내역은 인터넷이 가능한 스마트폰에 저장이 되어 있으며 이는 개인의 사적 관심사 혹은 근심을 알 수 있다. 이 중, 개인이 인터넷으로 질병에 대한 검색을 하면 고스란히 휴대폰에 해당 검색 내역이 저장되어 남는다. 또한, 휴대폰에 있는 자료를 토대로 개인이 어디에 있었는지 알 수 있다. 즉, 휴대폰에는 과거 위치정보(GPS 기반)가 저장되어 있으며, 이를 토대로 휴대폰 소지자의 동선을 분단위로 추적을 할 수 있을 정도이다.

스마트폰 어플리케이션(앱)[46]은 개인 삶의 모든 양상에 대한 상세한 정보를 제공한다. 이런 앱에는 민주당 뉴스, 공화당 뉴스가 포함

45) 동 보고서에 따르면, 미국 성인72%는 스마트폰을 5피트 범위내에서 대부분의 시간 항상 소지하고 다닌다고 조사가 되었다. 스마트폰 사용하는 장소로는, 9%는 섹스하는 동안, 12%는 샤워하는 사이에도 소지하고 있다고 설문 조사를 했다.

46) 손봉석 기자, "구글플레이, 앱 보유 개수 애플 앱스토어 추월", 경향신문, 2015. 1. 26.; 26일 모바일 시장 전문조사업체 '앱피겨스'에 따르면 구글플레이는 2014년 두드러진 성장세를 나타내며 시장 선두주자였던 애플 앱스토어를 추월했다. 구글플레이 앱 보유 개수는 2014년 기준 140만개로 전년도 70만개 대비 100% 성장했다. 이는 애플 앱스토어(120만개)의 116%, 아마존 앱스토어(28만개)의 500% 수준이다.
http://bizn.khan.co.kr/khan_art_view.html?artid=201501261719381&code=930100&med=khan

이 되어 있을 것이며, 알코올, 마약 그리고 도박 중독, 임신 심장박동에 대한 추적, 자산관리, 하고 싶은 취미생활, 당신의 로맨스를 증진시키는 앱 등 다양한 종류가 있다. 또한, 어떤 물건을 사고파는 대중적인 앱이 있으며, 이러한 기록은 휴대폰을 통해 접속하여 확인할 수 있다. 100만개 이상의 앱이 있으며 평균 일반 사람은 33개 이상 앱을 설치한다. 앱을 통하여 개인의 삶에 대한 몽타주를 작성할 수 있다.

과거에는 개인의 주머니를 뒤지는 것은 그 사람의 주거지를 수색하는 것과 전혀 비교를 할 수 없는 일이었다. 하지만, 만약에 개인의 주머니에 휴대폰이 들어 있으면 이야기가 달라진다. 휴대폰을 수사기관에서 수색하는 것은 개인의 주거지를 수색하는 것보다 훨씬 더 큰 피해를 주는 것이다. 휴대폰은 개인의 주거지에서 발견되는 많은 민감한 정보에 대하여 디지털 형태로 저장이 되어 있으며, 개인의 주거지에서 찾을 수 없는 광범위한 개인 정보를 담고 있다.

휴대폰이 문제를 더 복잡하게 하는 것은 휴대폰 자체가 단순히 디지털 정보 저장 매체 보관의 개념을 벗어나, 언제 어디서나 네트워크를 통하여 서버에 있는 저장 공간에 접속할 수 있다는 것이다(클라우딩 컴퓨팅[47]). 휴대폰 사용자는 자신의 데이터가 휴대폰 메모

47) 노윤재, "클라우드 컴퓨팅 환경을 이용한 개인정보보호 기술에 관한 연구", 고려대학교 박사학위논문, 2010.

클라우드 컴퓨팅의 개념은 2006년 구글에 재직 중이던 크리스토프 비시글리아가 처음 제안한 것으로 그는 당시 회사의 많은 컴퓨터가 완전하게 활용되지 않고 있다는 점에 주목하여 기업과 개인의 별도의 서버나 PC가 없어도 소프트웨어, 데이터 등을 온라인으로 저장해 두고 인터넷을 통해 임대해서 사용하자는 신개념을 발표하였다. 클라우드 컴퓨팅의 정의는 데이터센터 또는 대형 컴퓨터를 운영하는 전산센터를 클라우드라고 하며 네트워크 접속이 가능한 PC, 휴대폰, PDA등 다양한 단말기를 통해 장소와 상관없이 클라우드에 저장된 모든 소프트웨어 및 데이터를 이요하여 원하는 작업을 수행할 수 있는 컴퓨팅 기술이라 할 수 있다.

리에 저장이 된 것인지, 클라우드 서버에 보관이 된 것인지 명확히 모른다.

수사기관에서도 역시 체포현장에서 압수수색은 원격으로 접속하여 자료를 확보하는 것은 포함을 하지 않는 것이라고 인정하고 있다. 이러한 경우 범인으로부터 집 열쇠를 압수하여 그것을 통해 집을 수색하는 것과 같은 이치이다. 그러나, 수사기관에서 범인으로부터 휴대폰을 건네받아 기기 안에 저장되어 있는 자료를 검색하는 것이 해당 기기에 저장이 된 것인지 클라우드에 보관되어 있는 자료인 것인지 알 수 없다.

비록 수사기관에서 이러한 문제점을 인식하고 있지만, 수사기관에서 제안한 해결책은 불분명하다. 수사기관에서는 휴대폰을 수색할 때 데이터를 차단하고 수행을 하고 있다고 주장하고 있다. 이는 비단 이런 문제를 해결하는 것과 더불어 원격삭제를 방지하기 위해서 시행을 하고 있는 것이다. 대안책으로 수사기관에서는 클라우드 컴퓨팅으로부터 생성된 자료를 추출하는 기법을 발전시킬 것이라고 제안하고 있다. 물론 좋은 생각이지만 압수수색이 지나치게 광범위하게 이루어지는 것을 해결할 수 없을 것이다.

미국 수사기관에서는 어떤 특정한 상황에서 영장 없는 휴대폰 수색을 광범위하게 허용하고 있다. 하지만, 예외적인 상황을 살펴보면 대부분 오류가 있으며 법 위반적인 요소가 많이 있다. 수사기관에서는 상호 대립되는 이익형량에 대한 실행 가능한 규칙을 가지고 있으면, 반드시 단언적으로 되어 있어야 하고 케이스별로 그리고 담당 경찰관에 따라 변동이 되지 않아야 한다.

미국 수사기관에서는 최초로 'Gant' 표준을 만들었다. 위 표준에 따르면 현행범인이 체포된 범죄와 관련된 증거가 휴대폰에 저장이

되어 있다는 것에 대한 믿음이 합리적이면 영장 없이 휴대폰에 대하여 수색을 할 수 있는 것을 허용한다. 그러나, 위 표준은 휴대폰 수색과 관련하여 실질적 제한을 하나도 증명을 하지 못하고 있다.

수사기관에서 제안한 또 다른 규칙은 휴대폰 수색에 대한 범위 한정이다. 즉, 범죄와 관련되어 저장이 되어 있는 증거에 한정하여 수색을 할 수 있는 것이다. 그런데 해당 증거가 어디에 저장이 되어 있는지를 알 수 있는지 구별하는 것 또한 쉽지가 않다.

또한, 수사기관에서 언제든지 현행범으로 체포된 자의 휴대폰 통화기록을 볼 수 있다는 것에 대하여 반대한다. 휴대폰 통화기록은 단순한 통화기록만 저장되어 있는 것이 아니라 상대방 전화번호, 그리고 그 전화번호에 대하여 특정 이름을 표시한 것까지 알 수 있다. 본건에서는 피고인 Wurie가 'my house'라고 연락처를 저장하였다.

마지막으로 구두변론에서 수사기관은 다른 제안 원칙을 제안하였다. 즉, 수사기관에서는 만약 현행범인의 포켓 다이어리를 열어 소유자의 주소를 복사할 수 있으면, 반대로 현행범인의 휴대폰을 켜서 해당 전화번호를 알 수 있는 것은 합리적이라고 주장하고 있다. 하지만, 이는 디지털 형태 이전의 증거물에 대해서는 사진 촬영 몇 장을 압수할 수 뿐 이지만, 휴대폰에는 수천 장의 사진이 있을 수 있고 이에 대하여 같은 논리를 적용할 수 없는 것이다. 예를 들어 현행범인 주머니에 은행 이체내역 종이 1장이 있다고 하면, 반대로 현행범인의 휴대폰을 통하여 범인의 5년간 은행거래내역을 확인 할 수 있다는 논리인데, 이는 전혀 합당하지 않다. 더군다나 휴대폰에 저장되어 있는 자료는 그 종류에 있어 다양한 반면, 반대로 그와 같은 물건을 사람들이 출력물이나 물건으로 가지고 다니는 경우는 드물다.

또한, 어떤 디지털 파일이 물질적인 기록과 일치하는지 여부를 확인하는 것은 어렵다. 이메일이 편지와 일치하다고 볼 수 있을까? 보이스메일이 자동응답전화 메시지와 일치하는 것일까? 결국 수사기관이 수색을 수행하기 전에 이러한 종류에 대하여 일치하는지 여부를 결정하는 것은 명확하지 않다.

(사) 결론

우리는 오늘 우리의 결정이 수사기관이 범죄현장을 제압하는데 있어 영향을 미치는 것을 부인하지 않을 수 없다. 휴대폰에 저장되어 있는 통화기록을 통하여 범죄 조직의 조직원을 확인할 수 있으며, 휴대폰에 흉학 범죄에 대하여 기소할 수 있는 상당히 많은 증거를 제공하고 있다. 물론 개인 프라이버시는 그에 대한 값을 치러야 한다.

오늘 법원의 결정은 물론 수색에 있어 신성불가침이 아니고, 수색을 하기 전에 압수수색영장을 청구한 후 수색을 해야 된다는 것이다. 최근 기술 발전으로 영장신청을 하는 것이 효율적이 되었다(경찰관은 이메일 영장을 판사의 아이패드에 요청할 수 있고, 판사는 영장에 서명을 한 후에 다시 이메일로 경찰관에게 발송한다. 이렇게 하는 데 걸리는 시간은 고작 15분도 채 되지 않는다)[48]

더욱이 현행범인 체포현장에서 휴대폰의 압수수색은 허용되지 않

48) Recent technological advances similar to those discussed here have, in addition, made the process of obtaining a warrant itself more efficient. See McNeely, 569 U.S., at ‑‑‑‑‑‑‑, 133 S.Ct., at 1561‑1563; id., at ‑‑‑‑‑‑‑, 133 S.Ct., at 1573 (ROBERTS, C.J., concurring in part and dissenting in part) (describing jurisdiction where "'police officers can e-mail warrant requests to judges' iPads [and] judges have signed such warrants and e-mailed them back to officers in less than 15 minutes"').

지만, 다른 예외사유에서는 특정한 휴대폰에 대하여 영장 없이 수색을 할 수 있다. 예를 들어 수사기관이 긴급상황에서는 휴대폰을 수색하는 것은 수정헌법에 의거 정당화 된다. 긴급상황에는 개별적인 사건에서 증거인멸 같은 경우 해당될 수 있다. 그리고, 심각하게 부상당한 사람을 구조하거나 즉각적인 위해로 협박받고 있는 경우 적용이 될 수 있다. 판례에서도 수사관이 트렁크에 폭발물 같은 위험물이 들어 있을 것이란 합리적 믿음이 있으면 트렁크를 열어 보지 않은 채 경찰서로 운송하는 것은 무모한 것이라고 보았다. 이러한 긴급상황에서 영장 없이 휴대폰 등을 수색하는 것에 대하여 나중에 법원에서 긴급상황이 정당한 것으로 증명이 되어야 한다.

수정헌법은 미국 선구자의 일반영장과 가택수색영장(식민지 시대의 미국에서 식민지 상급 법원이 영국 왕의 임명을 받은 세관원에게 가택 수색의 권한을 부여한 명령장.) 에 저항에서 만들어 진 것이다.[49]

휴대폰은 단지 또 다른 기술적 편의사항이 아니다. 휴대폰에 저장하고 있는 것은 많은 미국인의 개인 프라이버시이다. 현대 기술로 상당한 개인정보를 손쉽게 휴대폰에 저장하고 다닐 수 있다고 해서

---

49) Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "'general warrants'" and "'writs of assistance'" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that "'[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance.'" 10 Works of John Adams 247–-248 (C. Adams ed. 1856). According to Adams, Otis's speech was "'the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born.'" Id., at 248 (quoted in Boyd v. United States, 116 U.S. 616, 625, 6 S.Ct. 524, 29 L.Ed. 746 (1886)).

그러한 정보가 선조들이 투쟁하여 지킨 보호할 가치가 없다는 것을 의미하지 않는다. 우리의 결정은 수사기관에서 체포현장에서 휴대폰을 수색하기 위해서는 법원의 영장이 필요하다는 것이다.[50]

(2) Westlaw 2014 WL 7793690(2014. 12. 30.)

미국 캔자스 주 법원은 수사기관의 휴대폰 압수수색 영장에 대하여 빈번히 기각 결정을 내리고 있다. 그 중 최근에 휴대폰 압수수색 기각을 한 판결문을 살펴보도록 하겠다.

(가) 사건 개요

수사기관(DEA, 미국 연방마약수사단속국)은 미국 캔자스 지방법원에 5개의 휴대폰에 대한 압수수색 영장을 청구하였다. 첨부된 선서진술서를 보면 수사기관에서는 위 5개의 휴대폰이 마약 거래에 있어 서로 전화연락을 하였고 그런 정황에 대한 증거가 들어있다면서 범죄 혐의 상당성이 있다고 주장하였다. 그래서, 수사기관에서는 위 휴대폰에 대한 수색을 허용하고 휴대폰에 저장된 이름, 주소, 전화번호, 문자메세지, 사진, 동영상, 혹은 사건과 관련된 다른 식별자

50) Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold *2495 for many Americans “"the privacies of life,”" Boyd, supra, at 630, 6 S.Ct. 524. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—-get a warrant.

료 혹은 통신자료에 대한 압수수색영장을 요청하였다.

(나) 기각 사유

현대 기술이 빠른 속도로 발전함에 따라 디지털증거에 대한 압수수색영장 발부시 수정헌법의 가치를 적용하는 것은 매우 어렵게 되고 있다. 대법원의 가이드라인 부재로 인해 미국 하급심 법원 상호간의 디지털 증거에 대하여 의견이 충돌되고 있는 상황이다. 이러한 충돌이 있음에도 압수수색 영장을 발부할 때, 개인의 프라이버시에 대한 보호와 수사기관의 범죄사실에 대하여 기소를 하는데 있어 효과적인 증거를 확보할 수 있는지 양자 간의 적절한 균형을 고려하는 것에 대해서는 의견의 일치를 보고 있다.

기술 발전이 급속도로 빨라짐에 따라 미국 주 법원이 부딪치게 될 다양한 사건에 있어 대법원 판결례는 아직 없고 앞으로도 계속 없을 것이다. 결과적으로 하급심 법원의 잘 정비된 규칙과 기술 영역에 있어서 필요한 것 사이에 눈에 띄는 간극이 발생하고 있다. 하지만, 법원은 이러한 간극이 수정헌법의 진실성과 목적에 대하여 타협하는 방편으로 법원이 결정을 하는데 있어 영향을 미쳐서는 안된다.

이어서, 앞서 살펴본 대법원의 Riley 판결문의 내용을 인용하면서 휴대폰에는 개인의 수많은 정보가 집적 되어 있고, 휴대폰을 압수수색 하는 것은 단순히 물건을 압수수색 하는 것하고 질적으로나 양적으로 차이가 분명한 것이라고 보았다. 추가로, 휴대폰은 다양한 디지털 기기(컴퓨터, 태블릿, 기타 다른 장치)와 연동이 쉽게 되어 사용상의 편리함이 있다. 편리성으로 인해 수사기관에서는 헌법상

허용되지 않은 무제한 압수수색 영장을 집행 할 수 있게 될 위험을 초래하고 있다. 연방 제10 항소법원은 문제점을 인식하여, 디지털 저장 매체는 이전의 저장 매체보다 훨씬 더 많고 다양한 종류의 정보를 저장하고 있기 때문에 컴퓨터는 수사기관의 유죄의 증거로 사용할 수 있는 탐나는 표적이 되고 있다고 보고 있다. 물론, 휴대폰은 컴퓨터 보다 수사기관한테는 훨씬 더 탐나는 표적이 되는 것은 분명하다. 휴대폰은 개인이 항상 소지하고 다니고 있으며, 상대적으로 계속사용을 하고 있으며, 거의 전원을 끄지 않고, 개인의 상호작용과 실시간 움직임에 대한 상세한 로그 파일을 가지고 있다. 이어서, 앞서 살펴본 대법원 판결에서 언급한 휴대폰이 클라우드 컴퓨팅과 연결되는 문제를 지적하였다.

제한 없이 이루어지는 영장의 다가올 위험은 수없이 많다. 예를 들어, 수사기관에서 혐의자의 컴퓨터 하드드라이브를 수색하고 싶으나 그렇게 할 상당성을 설명하지 못할 경우, 대신 휴대폰에 대한 압수수색을 청구할 것이다. 개인 디지털 기기는 네트워크로 연결이 되어 있고 클라우드로 상호 정보를 교환하고 있기 때문에 수사기관에서는 휴대폰을 통해 혐의자의 컴퓨터에 접근할 수 있다. 이렇게 하여 수정헌법에서 요구하는 상당성을 피해가는 것이다. 앞으로 이러한 영장의 폐해를 제한하기 위해서는 영장의 범위에 대하여 제한을 해야 한다. 제한이 없게 되면 말 그대로 수사기관에게 백지위임장을 주는 모양새가 된다. 수정헌법에서 요구하는 특정성은 디지털 증거에서 더욱 더 중요성을 가지게 되며, 법원은 디지털 증거 영장 발부시 특별한 주의를 기울여야 한다.

(다) 결론

법원에서 본건 영장을 발부하게 되면 수정헌법에서 요구하는 특정성을 부정하는 것이 된다. 본 영장을 발부하기 위해서는 개인 사생활의 보호라는 권리와 수사기관의 효과적인 증거수집이란 목적 상호간의 이익형량을 해야 한다. 수사기관에서는 디지털 증거 관련하여 어떻게 압수수색 하는지에 대한 방법(search protocol)에 대하여 설명을 해주어야 하고, 이를 통해 수사관이 선의와 수정헌법의 이념에 따라 압수수색을 하는 것인지 법원이 알 수 있고 법원은 해당 설명을 들어보고 영장 발부 여부를 검토할 수 있는 것이다. 이러한, 법원의 요구사항이 수사기관에게 부담이 된다고 믿지 않는다.

다) 압수방법 제한 부여 판례

미국 제9항소법원에서는 수사기관의 압수수색 영장 관련하여 압수방법 제한을 하거나 기타 다른 방법을 통하여 통제를 하고 있는 것으로 악명이 높다. 하지만, 모든 수사기관의 압수방법에 대하여 제한을 하는 것이 아니라 케이스별로 제한 조건을 부여를 하고 있다.

(1) Comprehensive Drug Testing, 579 F. 3d 989,(9th Cir. 2009)[51]

51) 이완규, 앞의 논문, 제 45~46면 각주

이 사건에서 수사기관은 10명의 프로야구 선수들의 약물복용 혐의와 관련하여 그들에 대한 테스트 결과를 찾기 위해 회사 사무실에 대한 압수수색영장을 받았는데 당시 치안판사는 영장에 기재된 자료를 분리하는 데 수사요원들 보다는 포렌식 전문가를 사용하라는 제한 등 몇 가지 제한을 부과하였다.

회사에서 영장을 집행하면서 포렌식 수사관들이 그 자료를 담고 있는 폴더를 찾았는데 그 폴더에는 10명에 관한 자료뿐만 아니라 다른 선수들의 자료들도 포함되어 있었다. 포렌식 수사관들은 컴퓨터 자체를 압수하는 대신에 폴더에 있는 파일들을 복사하였고 후에 수사요원들에게 그 파일을 교부하였다. 수사요원들은 10명의 혐의자들에 관한 결과를 찾기 위해 파일들을 검색하였고 그 과정에서 수백명의 다른 선수들의 결과들도 육안발견이론의 범위에서 보게 되었다. 이에 따라 이들 중 일부를 수사를 확대하는 데 이용하려 하였다. 메이저리그 야구선수 협회에서는 영장범위 밖에 있는 자료를 반환하라는 신청을 하였고 지방법원은 그 신청을 받아들였다. 이에 대한 항고심에서 3인 재판부는 지방법원의 결정을 파기하였는데, 재항고심의 전원합의체에서 항소심을 파기하였다.

이 판결에는 영장에 특정된 사항 이외의 것을 전체적으로 압수하는 것은 수정헌법 제4조에 부합하지 않는다는 점과 정부가 지방법원의 명령에 대한 항고기간을 지키지 못하였다는 점 등에 의해 지방법원의 명령을 유지하면서 추가적으로 “결론적 여론(concluding thoughts)”라는 장에서 치안판사들이나 수사기관이 혼합된 디지털 증거를 압수수색함에 있어 준수하여야 할 사항으로 몇 가지 기준을 제시하였다.

- 치안판사들은 정부로 하여금 디지털 증거 사건에 있어서는 육안발견이론의 원칙 적용을 포기하도록 요구하여야 한다.
- 치안판사는 다른 증거를 확인하지 않으면서도 영장 대상인 사항을 확인하기 위해 마련된 압수수색 집행 방식서를 요구하고 이를 준수할 것을 요구하여야 한다.
- 자료의 분리와 편집은 전문요원 또는 제3의 독립적인 사람에 의해 행해져야 한다. 만약 분리가 정부의 전문요원에 의해 행해지는 경우에는 영장청구시에 전문요원이 영장의 대상인 정보 이외의 다른 정보를 수사요원들에게 누설하지 않겠다는 점에 대한 동의를 받아야 한다.
- 정부는 관련성이 없는 증거는 즉시 반환하거나 폐기하여야 하며, 이와 같이 행하였다는 점에 대해 영장을 발부한 판사에게 알려야 한다.

5. 소결

디지털 증거 압수수색은 사건과 관련성이 있는 것에 범위를 한정하여 압수수색하는 것이 원칙이다. 하지만, 언제든지 위와 같은 원칙이 적용이 되는 것이 아니라 예외 규정이 있기 마련이다. 형사소송법 역시 단서 조항을 만들었고, 압수수색 현장에서 선별압수수색이 곤란한 경우 정보저장매체 원본을 압수할 수 있다고 규정하고 있다.

수사기관은 위와 같은 단서 조항을 근거로 휴대폰은 무조건 압수수색 현장에서 원본을 압수한 후 수사기관 사무실에서 증거 사본 작성을 하고 있다. 하지만, 미국 대법원 판결에서는 휴대폰은 일반

물건과 그 성질이 다르며 같이 취급을 할 수 없다고 판단하였으며, 이런 논리를 휴대폰 압수수색에 대입해 보면 휴대폰은 민감한 개인정보가 저장되어 있기 때문에 선별 압수수색에 주의해야 한다.

지금 당장 휴대폰 압수수색을 제한하고 현장에서 피압수자가 참여하여 선별 압수수색을 하라고 하는 것은 현 기술상 무리가 있다. 하지만, 언제까지 기술 한계로 예외를 둘 수는 없으며 수사기관에서는 하루 속히 휴대용 휴대폰 압수수색 도구 개발에 전념해야 할 것이다.

Ⅳ. 휴대폰 압수수색 및 분석 절차

1. 의의

휴대폰은 일반 디지털증거 압수수색과 대동소이한 방식으로 압수수색을 하고 있다. 휴대폰 역시 증거의 무결성, 동일성을 확보하기 위하여 피압수자의 제출 확인이나 봉인을 해야 하고 파일 추출 과정에서 참여권을 보장해야 한다.

휴대폰은 기종에 따라 차이가 있지만 대부분의 최근 휴대폰은 제조사에서 원격 삭제 기능을 지원하고 있다. 이 기능을 이용하여 피압수자는 수사기관이 자신의 휴대폰을 압수한 이후 위 서버에 접속해서 데이터를 삭제할 수 있다. 원격삭제를 방지하기 위해서 수사기관에서는 휴대폰 압수시 배터리를 분리하거나 애플 아이폰처럼 배터리가 분리되지 않으면 종료 기능 버튼을 통해 전원을 차단해야 한다.

일선 수사팀에까지 휴대폰 증거 분석 도구가 배포되어 있지 않다. 그래서, 일선 수사팀에서는 휴대폰을 위와 같은 절차를 통하여 압수한 이후에 관할 디지털포렌식팀으로 증거 분석 의뢰를 해야 한다. 포렌식팀에서는 수사팀으로부터 인계 받은 휴대폰을 봉인 해제한 후 증거 사본 작성을 한다. 이때, 봉인 해제 과정은 비디오 또는 사진 촬영하여 증거의 무결성을 확보한다. 또한, 당사자가 참관을 원하면 참여하에 증거 사본 작성을 한다.

이하에서는 휴대폰 압수수색 절차에 대하여 세부적으로 살펴보겠고, 휴대폰 분석을 통해 산출된 분석보고서의 실제 내용 및 문제점

에 대하여 알아보도록 하겠다.

2. 휴대폰 압수수색 절차

가. 원본 압수

휴대폰은 현재의 기술과 장비로는 압수수색 현장에서 사건과 관련된 전자정보를 출력 복사하거나 메모리 전부를 복제하는 것이 매우 곤란하다. 그래서 법원에서도 다음과 같은 이유로 압수수색 현장에서 휴대폰 기기 원본을 압수수색한 것이 적법하다고 판단하였다. ① 휴대전화는 공통된 운영체제(os)를 갖고 있지 아니하여 각 제조사마다 메모리를 복제하는 방법이 다르고, 같은 제조사의 제품이라고 하더라도 제품명에 따라 메모리를 복제하는 방법이 다른 경우도 많은 점, ② 이에 피압수자가 어떠한 휴대전화를 사용하는지 알 수 없는 수사기관으로서는 압수·수색 현장에서 압수하게 될 휴대전화에 적합한 소프트웨어나 장비를 구비하는 것이 용이하지 아니한 점, ③ 또한 휴대전화 메모리를 복제하는 경우, 삭제된 전자정보를 복원하고 범죄사실과 관련된 전자정보를 선별하여 압수하는 것이 기술적으로 가능한지 여부를 두고 논란이 있다고 보이는 점(피고인이 2013. 5. 22. 제출한 변론요지서에서 기재한 '특정 프로그램을 이용한 루팅(rooting)이나 탈옥(jailbreak)을 하여 전자정보를 복제하는 방법'은 비할당 영역의 일부 데이터가 손상되어 삭제파일을 복구할 수 없는 경우도 있다는 점에서 보편화된 기술이라고 보기 어렵다), ④ 전자정보의 경우 간단한 조작에 의하여도 쉽게 변경되고 훼손될 우

려가 크므로 저장매체에서 전자정보를 분리하여 추출함에 있어 원본과의 동일성을 보장받기 위하여 무결성과 진정성이 확보될 것이 요구되는 점 등을 종합하여 볼때, 압수·수색 현장에서 휴대전화의 내용을 확인하고 범죄사실과 관련된 전자정보만을 선별적으로 복제하는 것이 현저히 곤란하다고 보이므로, 일단 a의 휴대전화 자체를 압수하여 수사기관 사무실로 가져온 것은 적법한 것으로 보인다.[52]

나. 휴대폰 압수 방법

1) 원격삭제로부터 보호

최근 스마트폰은 각 제조사 별로 거의 대부분 원격삭제(Remote delete) 기능을 제공하고 있다. 구글은 제조사와 별개로 모든 안드로이드폰에 적용 가능한 원격 삭제 서비스를 제공하고 있다. 아이폰은 'www.icloud.com'에 접속하여 휴대폰 잠금, 초기화, 사이렌 울리기 기 기능을 제공한다. 접속 방법은 iCloud.com에 접속하여 애플 아이디로 접속해서 나의 아이폰 찾기를 클릭하여 아이폰 지우기를 실행하면 원격삭제가 이루어진다.[53]

---

52) 부산고등법원 2013. 6. 5. 선고 2012노667 판결

53) 애플아이폰 사용설명서(iOS 8.1 소프트웨어)를 보면, 원격삭제 기능에 대하여 아래와 같이 설명을 하고 있다.

> 나의 iPhone 찾기는 다른 iPhone, iPad 또는 iPod touch에서 나의 iPhone 찾기 무료 App(App Store에서사용 가능)을 사용하거나 Mac 또는 PC의 웹 브라우저를 사용하여 www.icloud.com/find에 로그인하여 iPhone의 보안을 유지할 수 있습니다. 나의 iPhone 찾기에는 iPhone을 잃어버린 경우 다른 사람이 사용자의 iPhone을 사용하지 못하게 막는 활성화 잠금이 포함되어 있습니다. 나의 iPhone 찾기를 끄거나 iPhone을 지우고 다시 활성화하려면 사용자의 Apple ID 및 암호가 필요합니다.
>
> 나의 iPhone 찾기 켜기. 설정 > iCloud > 나의 iPhone 찾기를 켜십시오.

가) 배터리 분리

휴대폰을 피압수자로부터 압수하면 곧바로 배터리를 분리한다. 피압수자가 원격 삭제 기능을 사용하기 위해서는 인터넷으로 해당 서버에 접속한 후 기능을 실행하면 불과 몇 분 만에 휴대폰에 저장된 데이터가 삭제될 수 있다. 그렇기 때문에 휴대폰을 압수하면 다른 압수수색이 종료가 되지 않았더라도, 우선적으로 휴대폰 배터리를 분리하여 전자파차폐 봉투에 봉인한 후 보관해야 한다.

휴대폰 배터리를 분리하기 위해서는 모델마다 약간의 차이점이 있고, 경우에 따라서는 조작자의 실수로 커버 등이 손상이 될 수 있다. 따라서, 배터리 분리를 어떤 방법으로 하는지 의문이 들 경우 사용자에게 배터리 분리 지시를 하거나, 배터리 분리 방법을 익힌 후 조치를 취해야 한다.

나) 배터리 일체형

중요사항: 나의 iPhone 찾기 기능을 사용하려면 iPhone이 유실되기 전에 나의 iPhone 찾기가 켜져 있어야 합니다. iPhone은 장비를 찾아 보호할 수 있도록 인터넷에 연결되어 있어야 합니다. 나의 iPhone 찾기 사용하기. iOS 장비에서 나의 iPhone 찾기 App을 열거나 컴퓨터에서 www.icloud.com/find로 이동하십시오. 로그인하고 장비를 선택하십시오.

- 사운드 재생: 벨소리가 진동으로 되어 있는 경우에도 2분 동안 최대 음량으로 사운드를 재생
- 분실 모드: 분실한 iPhone을 암호로 즉시 잠그고 연락할 전화번호를 표시하는 메시지를 보낼 수 있습니다. 분실 모드가 되면 Apple Pay에 사용한 신용카드 및 직불카드도 일시 정지됩니다
- iPhone 지우기: iPhone의 모든 정보 및 미디어를 지우고 초기 설정으로 복원하여 개인 정보를 보호할 수 있습니다. iPhone 지우기를 하면 Apple Pay에 사용한 신용카드 및 직불카드가 제거됩니다

애플 아이폰은 배터리가 휴대폰 기기에 내장되어 있기 때문에 배터리를 손쉽게 분리할 수 없다. 따라서, 전원키를 이용하여 전원을 차단해야 한다.[54]

다) 기타 방법

이외에도 유심칩을 분리하거나 비행기 탑승 모드로 전환하여 휴대폰이 외부와 통신하는 것을 차단할 수 있다. 만약 수사팀에서 전자파차폐 봉투를 소지하고 있으면, 휴대폰을 압수하는 즉시 차폐 봉투에 봉인을 하면 외부 통신을 막을 수 있어 원격삭제로부터 증거물을 보호할 수 있다.

2) 정보저장매체 등 제출 확인서 작성

정보저장매체 등 제출 확인서에는 제출자, 제출 일시・장소, 기기의 종류, 제조사, 모델명, 실사용자, 가입자명 등을 기재한다. 제출자에게 자료 추출 참관 여부를 반드시 확인하여 기재토록 조치한다. 참관 의사표시가 있는 경우, 사후에 디지털포렌식팀과 일정을 조정하여 수사팀에서 당사자에게 통보 한다.

위 확인서 1부를 사본하여 휴대폰 기기와 함께 디지털포렌식수사팀에 송부하고, 원본은 수사기록에 첨부한다. 확인서 양식은 아래와 같은 것을 사용한다.

54) 애플아이폰 사용설명서(iOS 8.1 소프트웨어)를 보면, 슬라이더가 나타날 때까지 잠자기/깨우기 버튼을 누르고 있다가 슬라이더를 드래그하면 전원을 끌 수 있다.

[그림 정보저장매체 등 제출 확인서][55]

【정보저장매체 등 제출 확인서】

피압수자(임의제출자)	성명 :
	생년월일 :
	연락처(전화번호) :
압수(임의제출) 일시, 장소 등	
전원차단 일시, 장소 등	
기기의 종류, 제조사·모델명	기기의 종류 : 제조사 : 모델명(S/N) :
(모바일의 경우) 실사용자, 전화번호, 사용여부 등	실사용자 : 가입자명 : 전화번호, 통신사 : ☐ 현재 사용하고 있는 기기임 ☐ 사용하고 있지 않은 기기임
※ 피압수(임의제출) 기기에 패스워드, 잠금해제 등이 설정되어 있을 경우 설정 해제된 상태로 송부하거나, 해제가 곤란하면 패스워드, 잠금해제해제 등을 직접 기재하여 송부 ▣ 패스워드 : ▣ 잠금해제해제 :	
- 작성일 : 20 . . . - 작성자 : 00검찰청 00부 검찰수사관 000 (서명) - 제출자 000 (서명)	

【이미징 등 참관 여부 확인】

위와 같이 압수 또는 임의제출된 정보저장매체등에 대하여 이미징 등 과정에 (☐ 참관하였음, ☐ 참관하지 않았음) 을 확인합니다.	
참관 예정자	성명 :
	생년월일 :
	연락처(전화번호) :
작성일 : 20 . . . 위 확인자(피압수자·임의제출자 등) : (서명)	

55) 대검찰청 디지털수사과에서 자체 만든 양식

3) 압수물 봉인

대검찰청 디지털 증거 수집 및 분석 규정(대검 예규 616호, 2012. 11. 6.) 제 15조(정보저장매체등의 압수수색검증)에 압수물 봉인에 대하여 설명하고 있다. 제1항 단서의 정보저장매체등의 압수・수색을 행하는 경우에는 별지 제1호 서식의 압수물 확인지를 작성한 다음, 압수대상 정보저장매체등에 부착하여 책임자등의 확인·서명을 받고, 별지 제2호 서식의 압수물 봉인지를 이용하여 봉인한 후, 위 책임자등으로부터 확인·서명을 받아야 한다. 다만, 긴급을 요하는 등 부득이한 경우에는 다른 형식으로 봉인한 후 확인·서명을 받을 수 있다.

[그림 압수물봉인지]

(별지 제2호 서식) <개정 2012. 11. 6.> 압수물봉인지

검찰 PROSECUTION SERVICE	압수물봉인지		
봉인일시		확인자	
해제일시		해제사유	
특이사항			
- 이 물건을 봉인합니다. - 권한 없이 봉인을 해제하여서는 안됩니다.			

4) 압수물 확인지 작성

압수물 확인지는 위 대검 예규 같은 조에 규정한 것으로, 압수일시·장소, 피압수자의 서명 등을 기재한 후 휴대폰이 들어 있는 전자파 차폐 봉투 뒷면에 부착을 한다.

[그림 압수물확인지]

〔별지 제1호 서식〕 <개정 2012. 11. 6.> 압수물확인지

압수물확인지		
요청부서/ 주임검사		
제조사/ 모델명		
S / N		
시스템시간	년 월 일 시 분	
압수일시	년 월 일 시 분	
압수장소		
사용자		
피압수자		참관인
압수자		
비 고		

5) 분석 요청

일선 수사팀에서는 압수한 휴대폰을 관할 디지털포렌식팀에 분석 요청을 해야 한다. 검찰 및 경찰 자체적인 내부 시스템을 이용하여 전자결재 혹은 내부 인트라넷 망을 통하여 디지털포렌식팀에 분석 요청을 한다.

디지털 증거의 무결성 및 증거 손상 방지를 하기 위해서, 휴대폰은 충격 방지 조치를 확실히 한 후에 등기나 인편으로 송부한다.

3. 휴대폰 증거 수집 방법

검찰, 경찰, 해경, 관세청 등 국내 수사기관에서는 휴대폰(스마트폰 포함) 분석을 위해서 (주)지엠디시스템의 모바일포렌식 도구에 전적으로 의존을 하고 있는 실정이다. 위 도구는 휴대용이 아니라 분석실에 설치를 해야 되기 때문에 현장에 휴대하여 증거 수집 및 분석을 할 수 없다.

수사기관에서는 압수영장 및 임의제출 형식으로 휴대폰을 압수하게 되면, 휴대폰 전원을 차단하고 배터리를 분리한 채 전자파차단 방지 봉투에 봉인을 하여 각 관할 디지털포렌식센터에 인계를 한다. 포렌식센터 모바일분석팀에서는 수사팀으로부터 인계 받은 휴대폰에 대하여 소프트웨어 도구, JTAG, 메모리 Chip-Off 방식을 이용하여 증거 사본을 작성한다.

가. 소프트웨어 방법

지엠디시스템에서 판매하는 'MD-Smart' 제품은 스마트폰의 데이터를 USB 연결방식, JTAG, USIM, Removable Disk에 대하여 증거사본을 작성할 수 있다. 제조사 홈페이지[56]를 보면, 데이터 통신 오류 자동 탐지 기능, 데이터 추출 보고소 출력 기능, 스마트폰 어플 분석기능, 스마트폰 패턴 Lock, 핀번호 암호 해석, 삭제 데이터 복원 기능, 삭제 데이터 카빙 기능이 있다고 설명을 하고 있다.

소프트웨어 방식은 루팅[57]을 통한 물리 이미지를 복제하는 것이다. 루팅을 통하여 관리자 권한을 획득한 후 다운로드/리커버리 모드로 부팅하여 플래시 메모리 장치를 비트 단위로 복제를 한다. JTAG 보다 데이터 복제 시간이 빠른 특징이 있다. 다운로드 모드는 스마트폰 펌웨어 업데이트를 위해 존재하는 것으로 안드로이드 버전에 따른 영향을 적게 받는다. 다운로드 모드에서 파티션 테이블 정보를 얻고 모든 파티션에 데이터를 read-only 방식으로 증거 사본 작성을 한다. 안드로이드 기기 제조사별 특징이 있으며, LG 안드로이드 제품은 볼륨 UP + 볼륨 DOWN 버튼을 동시에 누른 상태에서 USB 연결한다. 삼성 제품은 홈키+볼륨 DOWN 버튼 + 전원키를 동시에 누른 상태에서 이루어진다.

리커버리 방식은 제조사별로 통일된 방식을 사용하여 비교적 용이하다. 리커버리 모드는 ADB 명령어를 이용하여 증거 수집을 한

56) http://www.gmdsystem.com/index.php?mm_code=700&sm_code=717

57) 루팅이란 루트 권한을 얻기 위한 방법으로 안드로이드 시스템 등에서 설정한 사용자의 접근 제한을 무력화 시키는 방법이다. 스마트폰은 제품 출하시 일반 사용자 모드로 출시가 되기 때문에 시스템 관련 파일 편집 및 삭제 등을 할 수 없어 안드로이드 기기 저장장치 복제가 불가하다.

다. 포렌식 도구 별로 ADB, netcat 명령어를 이용하여 증거 수집하는 방식에 차이가 있다.

나. 물리적 방법(JTAG, 메모리 Chip-Off)

1) JTAG

JTAG은 제조사에서 휴대폰을 디버깅하기 위해 사용하는 표준 인터페이스로, 이를 이용하여 휴대폰의 CPU를 제어함으로써 휴대폰의 메모리를 수집할 수 있다. 하드웨어 표준인터페이스를 활용한 방법은 휴대폰에 대한 파손의 염려가 없어 직접 메모리 접근 방식에 비해 유리하며, 물리적으로 데이터를 획득할 수 있으므로 휴대폰 증거 수집시 가장 우선하여 사용되어야 한다. 그러나 휴대폰이 비정상동작을 하는 경우 수집이 불가능 할 수 있으며, 휴대폰 마다 다른 입력신호의 사용과 CPU의 차이로 인해 휴대폰의 모델에 따른 케이블 제작과정이 필요하여 모든 휴대폰에 적용하는데 어려움이 있다.[58]

JTAG 연결 방식은 각 제조사 제품별로 연결하는 방식이 차이가 있으며, 지엠디소프트 같은 회사에서 직접 휴대폰 등을 수집하여 역공학으로 JTAG 단자를 알아낸 후 소프트웨어에 적용을 한 것이다.

2) 메모리 Chip-Off

휴대폰의 플래쉬 메모리의 내용을 직접 수집하는 방법은 휴대폰의 기판에서 메모리를 떼어 내어 메모리 리더기를 이용하여 수집하

58) 백재환, “모바일 메신저 사용정보 분석을 통한 디지털 포렌식 기법 연구”, 서울대학교 석사학위논문, 2010

는 방법으로 포렌식 관점에서 가장 바람직하다고 할 수 있다. 그러나 휴대폰의 메모리 종류에 따른 별도의 수집 장비를 제작해야 하고 기판에서 메모리를 분리하는 과정이 필요하므로 휴대폰을 손상시킬 수 있다. 따라서 휴대폰이 손상되어 정상 작동을 하지 않는 경우를 제외하고는 사용하기에 어려움이 있다.[59]

지엠디소프트에서는 'MD-MR' 제품이 있으며, 휴대폰의 플래시 메모리를 제거하여 데이터를 추출하는 장비이다. 휴대폰이 고장/화재/침수/훼손 되어 케이블 연결이 어려울 경우 플래시 메모리를 직접 제거하여 데이터를 추출한다.

4. 휴대폰 증거 수집 결과

모바일포렌식 분석도구를 이용하여 삭제 데이터 등을 복원하면, 해당 도구에서 지원하는 분석보고서를 엑셀 및 pdf 파일 형식으로 자동으로 생성을 해준다. 현재 검찰에서는 지엠디시스템의 포렌식 도구에서 제공하는 자동생성 분석보고서를 각 수사팀에 제공한다.

가. 보고서 내용

1) 분석정보

분석보고서의 엑셀 파일 첫 탭에 분석정보가 있으며, 해당 휴대폰에 대하여 누가 분석을 했고 증거사본 일시 및 해시값 그리고 증거사본 방법을 알려주고 있다.

---

59) 한국정보통신기술협회, "이동전화 포렌식 가이드라인", 2007

[표 6] 모바일분석보고서 분석정보

항목	내용
분석자	
제조사	SAMSUNG
모델	SM-N900S
이미징 일시	2015/04/16 15:54:46
MD5	275AE6A400B4B8EA8C32D7391D7E35C7 (검증:275AE6A400B4B8EA8C32D7391D7E35C7)
이미징 방법	MoviNand
작성일	2015/04/16 20:10:29
언어	한국어(대한민국) - 949
시간대	Asia/Seoul
프로그램 버전	Build 20150330.14792

2) 정보

분석대상 휴대폰에 대한 각종 계정정보, lock pattern를 알려준다. 또한, 시스템 정보로 휴대폰 초기화 정보, 안드로이드 버전, 전원 차단 시간, 언어, 타임존, 국가, MAC주소, 휴대폰 번호, IMSI 번호, 내 정보(휴대폰 번호와 사용자 이름)[60], 유심정보, 인터넷 계정, 이메일 계정, 무선인터넷접속 목록, 인터넷에 자동으로 접속을 해주는 아이디와 비밀번호, SNS 등 계정정보 등 사용자에 대한 상세한 정보를 알려주고 있다.

60) 사용자가 유심을 변경하여 다른 휴대폰 번호를 사용할 경우 이전에 사용한 휴대폰 번호와 새로운 번호 모두 알려준다.

3) 통화내역, 전화번호부

사용자가 통화내역을 삭제하더라도 플래시메모리에 해당 정보가 저장이 되어 있으면 복원을 할 수 있다. 사용자의 통화내역으로 삭제여부, 수/발신 여부, 사용자 이름(사용자가 지정한 이름), 전화번호, 통화일시, 통화시간을 알려준다. 사용자가 전화번호 그룹 설정을 했으면 어떤 그룹이 있는지 보여준다. 전화번호부 역시 사용자가 삭제를 했더라도 메모리에 남아 있으면 복원을 해준다. 전화번호부에는 카카오톡 등의 연락처 또한 같이 보여준다.

4) 메시지

문자메세지, 카카오톡, 위챗, 틱톡 등의 삭제된 메시지를 포함하여 복원을 한다. 카카오톡은 ID 및 채팅방 번호가 몇 번인지 알려준다. 메시지로 사진 파일을 첨부해서 보냈으면 해당 사진에 대하여 하이퍼텍스트로 직접 사진을 볼 수 있도록 해준다.

문자메시지에서 사건과 관련된 중요한 단서가 다수 발견이 되며, 그와 동시에 사건과 전혀 상관없는 개인적인 메시지 대화 내용 역시 복구가 될 수도 있다. 개인으로서는 숨기고 싶은 사적인 내용이 휴대폰을 분석하여 복구가 되는 치욕적인 일이 발생할 수 있다.

5) 이메일

컴퓨터에서 웹메일을 읽게 되면 메모리상에 임시로 저장을 하기 때문에 컴퓨터 전원을 끄게 되면 해당 웹메일의 내용을 복구할 수

없다. 즉, 컴퓨터에서 웹메일을 복구하기 위해서는 메모리 덤프 방식으로 해야 되는데 쉽지 않다. 그것도, 압수수색 당일에 메모리에 남아 있는 웹메일만 확인을 할 수 있다. 하지만, 스마트폰은 웹메일이 플래시메모리에 저장이 되어 있는 경우를 종종 볼 수 있다. 그렇기 때문에 모바일포렌식 도구를 이용하여 메모리에 웹메일이 저장이 되어 있으면 해당 이메일 내용을 확인을 할 수 있다. 아래 그림은 모바일분석보고서의 이메일 내용 중 사용자를 특정할 수 있는 정보를 삭제하였고 메일 내용도 임의로 변경하여 샘플로 만들어 보았다. 이처럼, 오래 시간 전에 보낸 이메일의 내용을 알 수 있으며, 받은 이메일의 내용 역시 알 수가 있다.

[그림 5] 이메일 내용

이메일

상태	종류	발신	수신	날짜	내용
활성	Sent	ba2@naver.com ba	y@naver.com	2013/11/30 17:12:03	제목 : 연락바랍니다^^ 광고보고 남겨요~^^ 필로폰을 구입하려면 어떻게 해야 되나요 일단 연락함주실래요? 010 0000 0000 삼성 모바일에서 전송하였습니다
활성	INBOX	y@naver.com y	ba@naver.com	2014/02/04 16:12:58	제목 : 야한거 보낸다

6) 일정, 메모 등

사용자가 My calendar에 저장한 일정을 보여준다. 해당 일정이 언제까지 반복한 후에 종료하는지도 알려준다. 사용자가 휴대폰에 메모를 하여 저장을 하면 해당 메모 내용을 알 수 있다. 갤럭시 노트 s메모를 이용하여 저장한 메모 내용을 사진 파일로 제공을 해준다. 사용자가 할 일에 대하여 알람을 설정한 경우 메모 내용 및 기간, 알람 시간, 중요도를 보여준다.

7) 멀티미디어

통화녹음 파일, 사진 파일, 동영상 파일 목록을 보여주며, 해당 파일에 대하여 하이퍼링크를 제공한다. 휴대폰 관련사건 판결 내용은 멀티미디어 항목에서 복원된 다른 사건과 관련된 증거가 발견되어 문제가 생긴 것이다. 통화녹음 파일은 '통화녹음 010-0000-0000 001.amr" 형식으로 되어 있다. 그리고, 녹음을 한 시간 및 종료 시간을 같이 알려 준다.

그리고 스마트폰에 저장이 되어 있는 한글문서, 워드 문서가 있으면 위 멀티미디어 카테고리에서 같이 보여준다.

8) 인터넷 기록, 지도 기록 등

인터넷 접속 시간, 제목, URL, 방문횟수를 알 수 있다. 네이버 같은 포털사이트에서 검색을 한 경우 검색어를 알려준다.

스마트폰 네비게이션 Tmap 등의 위치 검색어를 알려준다. 하지만, GPS 시작 좌표 와 종료 좌표 정보는 내용을 알 수 없다. 구글스토어 마켓 검색어를 보여주고, 어플리케이션 최근 앱 시작 시간, 앱 종료 시간, 실행 횟수를 알려준다.

[그림 6] 마켓 검색어

기타

상태	종류	날짜	내용	비고
활성	마켓 검색어	2015/01/04 18:34:44	롯데카드	
활성	마켓 검색어	2014/12/31 00:56:55	요기요	
활성	마켓 검색어	2014/12/23 09:44:40	텔레그램	
활성	마켓 검색어	2014/11/06 13:39:29	전광판	
활성	마켓 검색어	2014/11/05 01:06:45	viewcam	
활성	마켓 검색어	2014/11/05 01:00:18	Vmeyesper	
활성	마켓 검색어	2014/11/26 08:07:10	소라넷	
활성	마켓 검색어	2014/10/02 07:36:32	커플각서	
활성	마켓 검색어	2014/10/02 07:51:28	택시어플	

[그림 7] 어플리케이션 정보

어플리케이션 정보

상태	이름	어플 상태	경로	버전	날짜	메모
활성			com.nbaimd.gametime.nba2011:0		최근 앱 시작 시각 : 2015/04/15 18:29:54 최근 앱 종료 시각 : 2015/04/16 09:35:02	실행 횟수 : 96
활성			com.shinhan.sbanking		최근 앱 시작 시각 : 2014/08/05 13:15:25 최근 앱 종료 시각 : 2014/08/06 23:01:35	실행 횟수 : 922
활성			com.kbstar.kbbank:0		최근 앱 시작 시각 : 2014/12/27 09:08:11 최근 앱 종료 시각 : 2014/12/27 13:16:44	실행 횟수 : 919
활성			com.always.sportsscore			실행 횟수 : 916
활성			com.smartlotte:0		최근 앱 시작 시각 : 2015/03/16 16:18:13 최근 앱 종료 시각 : 2015/04/06 09:35:01	실행 횟수 : 9
활성			sstream.app:0			실행 횟수 : 9
활성			com.coupang.mobile		최근 앱 시작 시각 : 2014/08/05 15:16:04 최근 앱 종료 시각 : 2014/08/06 23:01:34	실행 횟수 : 83
활성			com.kakao.talk		최근 앱 시작 시각 : 2014/08/06 23:19:46 최근 앱 종료 시각 : 2014/08/07 05:00:01	실행 횟수 : 8292

Ⅴ. 문제점과 개선방안

1. 사건 관련성 개념 혼란

앞서 살펴본 휴대폰 녹음 파일의 사건 관련성 판결문(대법원 2013도7101판결)을 통하여 수사기관 및 법원의 사건 관련성 입장 차이를 정리해 보도록 하겠다.

가. 수사기관 입장

수사기관은 사건의 효율적인 수사를 위하여 사건 관련성 개념을 폭넓게 해석을 하고 있다. 적법한 절차에 의해 압수수색한 자료에서 사건과 관련성이 없는 자료가 나오게 되면 추가 압수수색 영장을 발부 받지 않고, 해당 증거를 토대로 별건 수사를 인지한다. 수사기관에서는 새로운 범죄와 관련하여 증거가 발견되었는데, 아무런 수사도 하지 않는다고 하면 부적절한 처사로 보이는 것은 분명하다.

수사기관에서는 휴대폰을 적법한 절차에 의하여 압수수색을 하였고, 휴대폰에 저장되어 있는 녹음파일에서 압수수색 영장 범죄사실과 관련 없는 제 3자에 대한 추가 범죄 사실이 발견되었다. 이러한 경우 압수된 휴대폰 내에 녹음되어 있는 을과 K간의 대화부분은 현재 갑을 피의자로 하여 수사되고 있는 사건과 관련성이 있어 적법한 압수물이고, 그 압수물을 기초로 별건 범죄가 수사되는 경우 별도의 압수절차 없이(왜냐하면 현재의 사건에서 적법하게 압수되어 있으므로) 그 별건 범죄에 대한 증거로 사용할 수 있다고 할 것이

다.[61]

본건 항소심[62]에서 검사는 “이 사건 녹음파일의 내용과 이 사건 영장의 범죄사실은 3주 남짓의 근접한 시기에 제19대 국회의원 선거에서의 공천과 관련하여 금품수수 또는 약속에 관한 내용이고, 그 청탁의 매개자가 a, 청탁의 대상이 되는 공천위원이 t로 공통된다는 점에 비추어 볼 때, 이 사건 영장 기재 혐의사실과 동종·유사의 범행에 해당한다고 의심할 만한 상당한 이유가 있는 범위 내에 속하므로 이 사건 녹음파일을 압수한 것에 아무런 잘못이 없다고” 주장하였다.

나. 법원 입장

본건 항소심에서 검사의 주장에 대하여 판사는 “이 사건 녹음파일이 b에 대한 공소사실을 입증하는 간접증거로 사용될 수 있다는 것과 이 사건 녹음파일을 이 사건 영장 범죄사실과 무관한 피고인 g과 a 사이의 범죄사실을 입증하기 위한 증거로 사용하는 것은 별개의 문제이므로, 이 사건 b 녹음파일에 대한 압수가 적법하다고 하여 피고인 g,a에 대한 관계에서도 적법한 것은 아니다”라고 판단을 하였다.

상고심에서는 “이 사건 녹음파일에 의하여 그 범행이 의심되었던 혐의사실은 공직선거법상 정당후보자 추천 관련 내지 선거운동 관련 금품 요구・약속의 범행에 관한 것으로서, 일응 범행의 객관적 내용만 볼 때에는 이 사건 영장에 기재된 범죄사실과 동종・유사의

61) 이완규, “디지털 증거 압수수색과 관련성 개념의 해석”, 법조 2013. 11월호, 71면.
62) 부산고등법원 2013. 6. 5. 선고 2012노667 판결

범행에 해당한다고 볼 여지가 있다. 그러나 이 사건 영장에서 당해 혐의사실을 범하였다고 의심된 '피의자'는 피고인 2에 한정되어 있는데, 수사기관이 압수한 이 사건 녹음파일은 피고인 1과 피고인 7 사이의 범행에 관한 것으로서 피고인 2가 그 범행에 가담 내지 관련되어 있다고 볼 만한 아무런 자료가 없다"고 판단하였다.

법원에서는 압수수색 영장 범죄사실에 기재된 것에 한정하여 사건 관련성 개념을 해석하고 있다. 법원은 별도의 압수수색 영장을 발부 받아 해당 녹음파일을 압수를 해야 한다고 보고 있다.

다. 미국 실무 및 판례

미국 실무 및 판례를 보면 기본적인 이념은 해당 사건과 관련성이 있는 증거 파일에 한정하여 압수수색 영장이 효력을 미치는 것이며, 추가로 다른 범죄사실과 관련된 증거가 발견된 경우 명인법리(plain view)를 제외하고는 법원에 추가로 압수수색 영장을 청구해야 한다고 보고 있다.[63] 미국 법원에서도 2단계 절차[64]를 허용하고

63) 미국 연방 법무부 산하 연구기관인 'Office of Legal Education Executive Office for United States Attorneys'에서 2009년 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation'(범죄수사에 있어 디지털 증거 획득 및 압수수색 매뉴얼) 3번째 개정판을 발간하였다. 동 매뉴얼은 미국 수사기관을 위하여 디지털 증거 압수 및 분석을 위해 각종 법규 및 판례의 예시를 들고 있다. 매뉴얼 90페이지 포렌식 분석 카테고리에 새로운 영장의 필요성에 대하여 다음과 같이 설명하고 있다. "A single computer can be involved in several types of crimes, so a computer hard drive might contain evidence of several different crimes. When an agent searches a computer under the authority of a warrant, however, the warrant will often authorize a search of the computer only for evidence of certain specified crimes. If the agent comes across evidence of a crime that is not identified by the warrant, it may be a safe practice to obtain a second warrant."(하나의 개인 컴퓨터는 여러 종류의 범죄에 연루될 수 있다. 그래서 컴퓨터 하드드라이브는 다수 다른 범죄의 증거들이 포함되어 있다. 수사관이 영장에 의해 컴퓨터를 수색할 경우, 보통 압수영장은 어떤 특정된 범죄에 대한 증거만 검색하는 것으로 한정하여 발부가 될 것이다. 이런 경우 수사관이 영장에 기재되지 않은 범죄에 대한 증거를 발견한 경우 새로운 영장을 발

있는 것은, 압수수색 현장에서 디지털 증거의 특성으로 현장에서 관련성 있는 증거 파일을 찾는 것이 힘들기 때문에, 현장에서 해당 저장매체 원본을 압수한 이후에 수사기관 분석실에서 사건과 관련성 있는 파일을 수색을 하는 것을 허용하고 있는 것이다. 하지만, 법원에서는 분명히 2단계 압수수색에 있어서도 사건과 관련성 있는 파일에 한정하여 수색을 하는 것이지, 사건과 무관한 자료들까지 압수수색을 허용하는 것이 아니라고 못을 박고 있다. 왜냐하면 수사기관이 이러한 자료까지 압수할 수 있도록 허용하게 되면 포괄 압수수색 영장이 되기 때문이다. 즉, 압수수색할 장소 및 물건에 특정성을 요구하는 것에 반하게 되는 것이다.

Riley 대법원 판결에서는 현행 미국 압수수색 영장 프로세스를 예를 들면서, 경찰관은 이메일 영장을 판사의 아이패드에 요청할 수 있고, 판사는 영장에 서명을 한 후에 다시 이메일로 경찰관에게 발송한다. 이렇게 하는 데 걸리는 시간은 고작 15분도 채 되지 않는다고 했다.

라. 개선방안

수사기관에서는 실체적 진실 발견을 하기 위하여 수사의 효율성을 강조하고 있다. 하지만, 실체적 진실 발견과 더불어 중요한 것은

부 받아야 한다)

64) 수사기관에서 압수수색 영장을 청구할 때 청구서에 디지털 기기를 사본하거나 원본을 압수하여 분석실에서 추가 압수수색이 필요한 사유를 상세히 기술을 하게 되면, 대부분 미국 법원에서는 압수 현장에서 디지털 기기를 압수 수색 하는 것은 시간이 많이 소요되고 오히려 피압수자에게 피해가 가는 것을 방지하기 위하여 2단계(two-step) 압수수색 절차를 허용하고 있다. 즉, 압수수색 현장에서 증거를 이미징하거나 원본을 압수한 후 디지털포렌식 분석실에서 증거물을 추가로 수색(탐색, search)을 하는 것이다.

적법절차 준수와 개인 사생활 보호 측면이다. 현행 형사소송법에서는 피고 사건과 관계가 있는 것에 한정하여 압수수색을 허용하고 있고, 여기서 피고 사건은 압수수색영장 청구 당시 범죄사실에 기재한 사건을 지칭하는 것이다. 또한 개인 사생활 측면에서 디지털 증거에는 사건과 무관한 사적인 자료가 많이 저장되고 있음에도 수사기관에서는 기술의 한계로 디지털 저장 매체 원본 자체를 압수하는 것이 정당화되고 있다.

1) 압수수색 대상에 전자정보 개념 추가 도입

앞서 살펴보았듯이 미국, 유럽평의회, 프랑스, 일본, 영국에서는 전자정보에 대한 압수수색을 허용하고 있다. 미국 수사실무를 보더라도 압수수색을 법원에 청구하기 전에 특정 전자정보가 필요한 것인지, 전자정보가 들어 있는 디지털 저장매체가 필요한 것인지에 대하여 판단 후 영장을 청구해야 한다고 기술하고 있다.

우리나라 형사소송법을 보면 압수의 목적물로 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체인 경우 기억된 정보의 범위를 한정하여 복제 및 출력을 해야 한다고 규정하고 있다. 즉, 사건과 관련성이 있는 것에 한정된 증거 파일만을 선별하여 압수수색을 해야 한다고 정하고 있는 것이다. 형사소송법 제 106조3항을 보면 컴퓨터 정보저장매체에 저장되어 있는 파일을 압수수색 하는 것처럼 보일 수 있다. 하지만, 명문에 압수수색 대상 종류에 컴퓨터용디스크, 기타 정보저장매체, 전자정보를 명시해야 한다.

법원에서 디지털증거에 대하여 압수수색 영장을 허용하는 것은 정보저장매체에 들어 있는 전자정보를 압수수색 하는 것을 의미하

는 것이다. 디지털 증거는 매체독립성이 있기 때문에 저장장소를 불문하고 해당 내용이 중요한 것이다. 하지만, 수사 현실에서는 전자정보를 선별하여 압수수색하는 것은 여러 어려운 점이 있기 때문에 디지털저장매체 원본 자체를 압수수색 하는 것을 단서 조항으로 허용하고 있는 것이다.

앞에서 언급한 관련성 없는 휴대폰 압수수색 판결을 살펴보면, 대법원은 수사기관이 다른 사건에 연관된 증거를 발견한 경우 추가 압수수색 영장을 법원에 청구하라고 언급을 하고 있다. 하지만, 현재 형사소송법의 압수 대상 적격으로는 물건만 해당이 되고 있기 때문에 수사기관이 기존에 적법하게 발부한 압수수색 영장으로 압수한 물건에 대하여 재차 압수수색 영장을 청구하라는 것은 법리적으로 맞지 않다. 그렇기 때문에 법리적으로 문제를 해결하기 위해서는 전자정보가 압수수색 대상 적격이 되어야 한다.

2) 2차 영장 청구 방식 변경

형사소송법이 개정되어 압수수색 대상에 물건, 전자정보가 포함이 될 경우, 수사기관에서는 적법하게 압수수색한 1차 영장으로 획득한 디지털 저장매체에서 영장 범죄사실과 관련 없는 제 3의 범죄사실에 중요한 증거가 발견된 경우 압수수색 영장은 어떻게 해야 하는가. 기존 압수수색 영장에 따라 법원에 청구하게 되면 법원 실무상 검찰 압수수색 영장은 영장전담판사가 발부를 하고 사경에서 신청한 경우 당직 판사가 발부를 하기 때문에 최대한 빠른 시간 안에 발부된다고 해도 청구일 다음날 오후 4시에 발부가 된다. 그렇다면,

시급을 요하는 사건에 있어서 기왕 압수수색한 물건에 대해서도 같은 절차로 압수수색 영장을 발부하는 것은 수사의 효율성 및 실체적 진실발견에 너무 저해 요소가 된다.

미국 사례에서 언급한 것처럼 경찰관이 치안판사의 아이패드로 영장을 청구하여 15분 만에 발부가 되는 것을 곧바로 도입을 할 수는 없을 것이다. 최초 영장을 청구하게 되는 경우 사건 기록을 판사가 보고 영장 발부 여부에 대하여 검토를 할 수 있다. 하지만, 2차 영장 청구에서는 사건 기록을 굳이 판사가 보지 않더라도 기존에 발부한 자료가 법원에 남아 있기 때문에 이를 토대로 수사기관에서 새롭게 발견된 증거에 대한 범죄사실을 기재하여 추가 압수수색 영장을 빠른 시간 안에 할 수 있는 방법을 찾아야 한다.

법무부에서는 법원 및 수사기관 상호간의 시스템을 통합하여 형사사법정보시스템(KICS)을 구축하여 운영을 하고 있다. 위 킥스 시스템에서 전산으로 새롭게 발견된 증거에 대한 범죄사실 및 발견하게 된 경위 등에 대하여 소명을 한 자료를 킥스로 법원에 발송을 하면, 영장 판사는 원 사건 기록 없이 충분히 영장 발부 여부에 대하여 판단을 할 수 있으면 빠른 시간 안에 영장이 발부될 수 있을 것이다. 혹여 최초 영장 발부 시점으로부터 상당 시간이 흐르거나, 판사가 영장 발부여부에 대하여 사건 기록을 요구하는 경우는 기록을 법원에 보내야 한다. 사건 기록이 없더라도 충분히 판사가 영장 발부 여부를 결정할 수 있도록 수사기관에서는 소명자료를 충실히 작성을 해야 할 것이다.

2. 휴대폰 압수수색 및 분석 관련 개선방안

가. 의의

스마트폰 이용자가 급격하게 증가하는 추세에 있고, 거의 전국민이 스마트폰을 사용하고 있는 환경에서 스마트폰에 저장되어 있는 각종 자료는 수사기관에 입장에서는 금광과 같은 존재이다.

법원에서도 사건의 특성상 휴대폰에 대한 압수수색은 한정하여 영장을 발부해 주고 있다. 이와 같은 이유는 휴대폰에는 개인의 사생활과 밀접하게 관련되어 있는 정보가 무궁구진하게 저장이 되어 있으며, 이와 같은 자료를 수사기관에서 볼 수 있는 것을 배제한 것이다. 실제 수사기관에서는 컴퓨터에서 보다 스마트폰, USB메모리 등 소형 정보저장매체에서 사건과 관련되어 중요한 증거를 발견하는 경우가 많이 있다. 그리고 외국에 비해 국내 스마트폰 분석 기술이 높은 수준에 있다. 외국과 달리 우리나라는 최초 관심을 가진 분야가 휴대폰에서 삭제된 데이터를 복구하는 것이었다. 그래서, 휴대폰을 복원하게 되면 심한 경우 피압수자가 중고로 구입한 휴대폰에 그 전 주인이 사용한 사진, 동영상, 문자메세지 내용까지 복원이 되는 경우도 종종 있다.

앞서 살펴본 휴대폰 관련 항소심의 판결문을 보면 휴대폰에 대하여 압수수색 현장에서 증거 사본 및 사건과 관련된 파일을 현장에서 할 수 없고 수사기관 사무실에 와서 분석을 한 것을 적법하다고 판단하였다.

나. 개선 방안

1) 필터링 필요

현행 수사실무를 살펴보면 디지털포렌식팀에서는 사용자의 휴대폰에 저장되어 있는 모든 자료를 수사팀에 제공을 해주고 있다. 수사팀에서는 이러한 사용자의 정보를 바탕으로 사건과 관련성이 있는 자료를 검색한다. 주로 메시지 내용에 저장되어 있는 대화 내용을 위주로 검색을 하는데, 휴대폰 사용자에 따라 카카오톡 등 메시지 내용이 방대하게 많을 수 있다. 방대한 데이터 중에 특정 사용자 상호 간에 주고받은 메시지를 필터링 하는 것은 손이 많이 가고 시간이 많이 걸린다. 더군다나, 그런 과정 중에 사건과 필요 없는 불필요한 개인 정보 또한 볼 수 있기 때문에 현재 수사실무에서 하고 있는 방법을 개선해야 할 필요성이 있다.

2) 필터링 예시 및 문제점

엑셀 형태로 저장되어 있는 모바일분석보고서의 문자메세지 중 사건과 관련되어 있는 사용자 상호간의 문자메세지를 선별하는 작업 예시를 들어보기로 한다.

문자메세지는 송수신 시간으로 정렬한 후 수신자의 특정 번호로 필터링한 후 새로운 엑셀 탭에 선택하여 붙여넣기를 한다. 이후, 다시 돌아와서 발신자의 특정 번호로 재차 필터링하여 조금 전에 붙여 넣은 마지막 행에 같은 방식으로 붙여넣기를 한다. 그리고나서, 메시지 송수신 내역 시간으로 정렬을 하면 특정 대상자 2명 상호간

의 문자메세지 송수신 내용을 확인할 수 있다.

하지만, 메시지 항목에는 문자메세지 뿐만 아니라 카카오톡, 위챗 등 SNS 메시지 내역까지 시간 순으로 같이 들어가 있다. 그런데 카카오톡은 수신/발신이 정확하게 들어가 있지 않아서 필터링을 하는데 어려움이 있다. 물론, 시간순으로 모두 정렬하여 일일이 내용을 확인하여 대상자 상호간의 카카오톡 대화 내용을 추출하면 되는데, 메시지 내용의 양이 적은 경우는 가능하지만 통상 카카오톡 대화 내용이 많이 있기 때문에 시간 및 노력이 많이 소요된다.

아래 표는 카카오톡 ID : 4746, 15527 사용자간의 대화 내용이다. 아래 대화 내용은 ID 4746 사용자의 휴대폰에서 추출한 카카오톡 대화 내용의 일부이다. 연번 1~2는 ID 4746 사용자가 ID 15527 사용자에게 보낸 메시지인데, 종류에는 수신으로 기재가 되어 있고, 연번 3~5번은 수/발신이 올바르게 적용이 된 것을 알 수 있다. 하지만, 연번 6~7번은 ID 4746 사용자가 보낸 메시지인데 수신으로 잘못 기재가 되어 있는 것을 알 수 있다.

[표 7] 모바일 분석보고서 중 카카오톡 예시

연번	상태	종류	발신자	수신자	날짜	내용	비고
1	활성	수신	발신자: ID:4746		2014/09/20 20:04:42	앞면이 없데	앱이름:카카오톡 채팅방번호:9243
2	활성	수신	발신자: ID:4746		2014/09/20 20:04:53	뒷면은 똑같아	앱이름:카카오톡 채팅방번호:9243
3	활성	수신	발신자:		2014/09/20	또왔어 엔조	앱이름:카카오톡

			ID:15527		20:06:01	이2	채팅방번호:9243
4	활성	발신		ID: 4746,15527	2014/09/20 20:06:15	상줘야겠네ㅋㅋㅋ	앱이름:카카오톡 채팅방번호:9243
5	활성	수신	발신자: ID:15527		2014/09/20 20:06:50	어떡하지	앱이름:카카오톡 채팅방번호:9243
6	활성	수신	발신자: ID:4746		2014/09/20 20:07:26	내가 봤을때 썸느낌나는데	앱이름:카카오톡 채팅방번호:9243
7	활성	수신	발신자: ID:4746		2014/09/20 20:07:38	계속오는거보니까	앱이름:카카오톡 채팅방번호:9243
8	활성	수신	발신자:ID: 155273162		2014/09/20 20:07:46	둘이 사랑하나?	앱이름:카카오톡 채팅방번호:9243

분석도구에서 이러한 오류가 발견이 되고 있기 때문에 특정 사용자 상호간의 대화 내용을 필터링 하는 것이 무척 힘이 들다. 수사기관에서는 모바일 분석 도구 제조업체에 건의하거나 자체 분석프로그램을 작성하여 메시지 대화 내용 중 특정 번호 및 아이디 상호간의 메시지 송수신 내역을 필터링 할 수 있는 기법을 도입해야 한다.

3) 필터링팀(Filtering Team) 운영

미국 제9항소법원에서는 수사기관의 압수수색 영장 관련하여 압수방법 제한을 하거나 기타 다른 방법을 통하여 통제를 하고 있다. 2009년 미국 프로야구선수 약물복용 사건에서 법원은 “① 자료의

분리와 편집은 전문요원 또는 제3의 독립적인 사람에 의해 행해져야 한다. 만약 분리가 정부의 전문요원에 의해 행해지는 경우에는 영장청구시에 전문요원이 영장의 대상인 정보 이외의 다른 정보를 수사요원들에게 누설하지 않겠다는 점에 대한 동의를 받아야 한다. ② 정부는 관련성이 없는 증거는 즉시 반환하거나 폐기하여야 하며, 이와 같이 행하였다는 점에 대해 영장을 발부한 판사에게 알려야 한다.[65]고 압수수색 방법에 제한을 했다.

우리나라 수사실무를 살펴보면 일선 수사팀에서 휴대폰을 압수수색 후 거점 디지털포렌식센터에서는 위 휴대폰을 인수 받아 증거사본 작성 후 분석보고서 형태로 휴대폰에 저장된 모든 데이터를 엑셀 및 pdf 보고서 형태로 저장을 한 후 수사팀에 인계를 하고 있다.

수사팀에서는 인력의 한계(검사실 근무 인원 검사 1명, 참여수사관 1~2명, 실무관 1명)로 인해 포렌식센터에서 건네받은 파일의 내용을 그대로 출력하거나 CD에 저장하여 사건 기록에 편철을 하고 있다. 설령 위 보고서의 모든 내용을 수사관이나 검사가 낱낱이 살펴본다고 가정을 하더라도 수사관 등은 사건과 전혀 별개의 문자메세지 등에 노출이 될 것이며 피의자에 대한 선입견을 가질 수 있다. 심한 경우 예를 들어 문자메세지에 저장되어 있는 피의자의 불륜메시지를 통해서 피의자와 사건 관련 협상을 할 수도 있으며, 이를 통해 자백을 이끌어 내는 비신사적인 수사가 이루어질 수 있다.

이를 방지하기 위해서 미국 연방항소법원에서 제안하는 필터링팀을 적극 도입할 필요성이 있다. 수사팀과 별개의 포렌식팀에서 위와

65) 이완규, "디지털 증거 압수수색 관련성 개념의 해석", 법조, 2013. 11월호, 제 45~46면 각주

같은 필터링을 하는 것이 바람직하며, 추가로 포렌식팀 인원이 증원되어야 한다.

하지만, 포렌식팀 인원 증원에는 한계가 있기 때문에 고도화된 필터링 기법 기술 개발이 추가로 필요하다. 일선 수사팀에서는 모바일 분석요청시 어떤 자료가 필요한지 상세하게 요청서에 작성을 해야 한다. 이를 바탕으로 필터링팀에서는 휴대폰에 저장되어 있는 자료 중 사건과 관련성 있는 자료를 선별하여 추출할 수 있을 것이다.

Ⅵ. 결론

디지털 증거는 저장 매체의 대량화로 인해 사건과 관련 없는 파일이 혼재가 되어 있다. 의사처럼 정확하게 상처 부위에 대하여 메스를 이용하여 병을 치료하면 가장 좋은 방법일 것이다. 하지만, 디지털 증거의 현실에서는 의사처럼 정교하게 사건과 관련이 있는 파일을 선별 작업을 하는 것은 사실상 불가능에 가까운 일이다. 이러한 현실을 반영하여 미국에서는 2단계 압수수색을 허용하고 있으며, 디지털수사요원이 2차로 분석하는 행위를 수색의 연장선상에서 보고 있다. 하지만, 미국 판례 및 실무에서는 디지털 증거의 특성상 2단계 압수수색을 허락을 하고 있지만 추가 분석 과정에서 사건과 관련이 없는 증거 파일이 발견된 경우 추가로 법원에 영장을 청구해야 한다고 보고 있다. 단, 명인법리(plain view)에 따라 일부 증거로 인정되는 경우도 있지만 안전하게 추가 영장을 발부 받으라고 수사실무에서는 권고하고 있는 실정이다.

최근 대법원의 입장 역시 수사기관이 정당하게 압수한 휴대폰에서 압수수색 영장 범죄사실에 적시한 이외의 추가 범죄사실이 발견된 경우 추가로 압수수색 영장을 발부 받아야 한다고 판단하고 있다. 수사기관에서는 위와 같은 대법원의 입장에 대하여 반발을 하고 있다. 법원에서 사건 관련성을 너무 협의로 보고 있다면서 수사의 신속성 및 효율성을 저해하는 처사이며 현행 압수수색 대상을 물건만 할 수 있는 현실에서 정당하게 압수하여 수사기관이 보관하고 있는 물건에 대하여 추가 영장을 발부 받으라는 것은 법리에 어긋난 행위라고 주장하고 있다.

하지만, 법원에서 디지털저장매체 압수수색영장을 발부해준 취지

는 영장판사가 해당 범죄사실과 관련하여 증거물이 디지털기기에 저장이 되어 있을 상당성이 있다고 본 것이다. 즉, 압수영장의 실제적 효력은 기기가 아니라 사건과 관련된 증거 파일 자체에 미치는 것이고, 사건과 관련이 없는 다른 파일에는 효력이 없는 것이다.

앞으로 수사기관에서는 영장 범죄사실과 다른 증거가 발견되면 추가 영장을 법원에 적극 신청해야 한다. 빠른 시일 안에 형사소송법이 개정되어 압수수색의 대상으로 전자정보를 추가로 압수 대상으로 되기 전까지는, 법원과 사전 협의를 하여 2차로 신청하는 영장에 한정하여 전자정보에 대한 압수수색 영장이 가능하도록 해야 할 것이다.

스마트폰은 디지털포렌식의 금광이라고 불릴 정도로 사건과 관련하여 중요한 증거가 많이 발견되어 기소에 상당히 도움을 주고 있다. 하지만, 그에 비례하여 스마트폰에는 사건과 관련이 없는 개인 사생활에 민감한 여러 많은 데이터를 저장하고 있다.

2014년 미국 대법원의 Riley 판결에서 법원은 휴대폰은 단지 또 다른 기술적 편의사항이 아니고, 휴대폰에 저장되어 있는 것은 많은 미국인의 개인 프라이버시라고 보았다. 그리고, 현대 기술로 상당한 개인정보를 손쉽게 휴대폰에 저장하고 다닐 수 있다고 해서 그러한 정보가 선조들이 투쟁하여 지킨 보호할 가치가 없다는 것을 의미하지 않는다고 보았다. 미국 법원에서도 기존에는 디지털 증거 관련 2단계 압수수색을 허용하였고, 일부 항소법원에서는 압수수색 방법을 제한하기도 하고 있다. 하지만, 대법원에서 휴대폰은 일반 물건 압수와 전혀 별개의 것으로 보고 있는 상황에서 추후 휴대폰에 대한 압수수색은 2단계 절차로 하는 것을 금지할 것으로 보인다.

국내 수사기관에서는 피의자로부터 휴대폰을 영장이나 임의제출 받는 형식으로 압수한 후, 포렌식수사관이 국내 독점 제조업체에서 제공한 도구를 이용하여 증거 사본 작성을 한다. 이후, 해당 도구에서 제공하는 분석보고서(엑셀,pdf)를 일선 수사팀에 제공을 한다. 즉, 포렌식수사팀은 사건 관련된 문자메세지, 카카오톡을 필터링하지 않고 전체 모든 내용을 수사팀에 제공을 한다. 수사기관에서는 내부 지침이 없는 상황에서 수사관별로 관련성 있는 파일에 한정하여 별도 파일을 작성하여 출력을 하거나 CD에 저장하여 기록에 편철을 하지만, 대부분의 수사관은 선별 작업하는 것이 번거로워서 전체 내용을 인쇄하거나 CD에 저장을 한다. 이렇게 되면 사건과 관련이 전혀 없는 피의자의 개인정보가 고스란히 사건 기록에 남게 된다. 이러한 관행은 분명 개인정보보호법에 위배되고 형사소송법에 규정한 압수수색 방법에도 맞지 않으며, 또한 헌법에서 보장하고 있는 사생활의 비밀과 자유, 정보자기결정권에 어긋난 일이다.

이를 방지하기 위해서 수사팀과 별도의 필터링팀을 운영하여 사건과 관련된 자료에 한정하여 선별 압수수색할 수 있도록 해야 한다. 필터링팀은 기존 디지털포렌식센터의 인력을 증원하여 운용하는 것이 적절하다. 수사기관과 전혀 별개의 민간기관에서 하게 되면 수사 보안 등 여러 문제가 발생할 수 있다. 필터링팀 운영과 더불어 고도화된 필터링 기법 기술 개발이 추가로 필요하다.

마지막으로 본 논문이 디지털증거 압수수색 실무를 함에 있어 미약하게나마 도움이 되기를 바라면서, 이 논문을 기초로 보다 더 많은 압수수색 실무에 대한 문제점을 발굴하여 수사의 효율성 및 개인의 인권보장 양 측면을 만족시킬 수 있는 계기가 되길 바란다.

참고문헌

Ⅰ. 국내자료

고려대학교 산학협력단, “외국판례에 나타난 디지털증거 수집·분석·보존 과정에서의 무결성 논란에 비추어 본 디지털 증거의 활용방안”, 대검찰청, (2006)

김익현 기자, “아이폰, 얼굴만 갖다 대면 바로 잠금 해제?”, ZDNET KOREA, 2015. 4. 1.
[http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150401081022]

노윤재, “클라우드 컴퓨팅 환경을 이용한 개인정보보호 기술에 관한 연구”, 고려대학교 박사학위논문, (2010)

대검찰청, “차세대 디지털 포렌식 기술 및 사이버범죄 대응 기술 연구”, (2012)

박상준, 서울대학교 수리정보과학과, “디지털포렌식 강의자료집”, (2015)

박종석, “해킹과 침해대응 메모리 포렌식”, 서강대학교 정보통신대학원, (2013)

백재환, “모바일 메신저 사용정보 분석을 통한 디지털 포렌식 기법 연구”, 서울대학교 석사학위논문, (2010)

서울서부지방검찰청, “신정아 변양균 사건 관련 중간수사 결과 발표자료”, (2007)

손동권, “수사절차상 긴급 압수·수색 제도와 그에 관한 개선입법론”, 경희대학교 법학연구소, <경희법학> 46권3호, (2011)

손봉석 기자, “구글플레이, 앱 보유 개수 애플 앱스토어 추월”, 경향신문, 2015.1.26.
[http://bizn.khan.co.kr/khan_art_view.html?artid=201501261719381&code=930100&med=khan]

신소영 기자, “[취재수첩] 왜 영장주의인가”,법률신문2013. 6. 13. 법률신문 2013.6.13.
[https://www.lawtimes.co.kr/Legal-News/Legal-News-View?Serial=75759]

오기두, “관련성 없는 휴대폰 녹음 파일 압수와 위법수집증거”, 법률신문 2013.3.4.

위재민, “형사절차법”, 대검찰청 내부 게시판 (2010)

이상우 기자, “이건 어디서 찍은 사진? 사진 속 위치정보 분석”, IT 동아, 2014.10.8. [http://it.donga.com/19427/]

이상우 기자, “컴퓨터와 휴대전화의 만남 스마트폰”, IT 동아
[http://navercast.naver.com/contents.nhn?rid=122&contents_id=4128]

이숙연, “전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여”, 헌법학연구 제18권 제1호, (2012)

이완규, “디지털 증거 압수수색과 관련성 개념의 해석”, 법조 11월호, (2013)

전승수, “디지털 정보에 대한 압수수색영장의 집행”, 법조 7월호, (2012)

지엠디시스템 홈페이지, [http://www.gmdsystem.com/]

한국정보통신기술협회, “이동전화 포렌식 가이드라인”, (2007)
한글과 컴퓨터, “HWP 5.0 파일포맷”, [http://www.hancom.com/]

Ⅱ. 국외자료

Jumio, "mobile consumer habits study", june (2013)
Office of Legal Education Executive Office for United States Attorneys, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation", (2009)
Zack Whittaker, “Smartphones ’remotely wiped’ in police custody, as encryption vs. law enforcement heats up”, ZDNet, 2014. 10. 9.
[http://www.zdnet.com/article/smartphones-remotely-wiped-in-police-custody-as-encryption-vs-law-enforcement-heats-up/]

Ⅲ. 판례자료

헌법재판소 2005. 5. 26. 선고 99헌마513, 2004헌마190(병합) 결정
대법원 2004. 3. 23. 선고 2003모126 결정
대법원 2007. 12. 13. 선고 2007도7257 판결
대법원 2011. 5. 26. 선고 2009모1190 결정
대법원 2012. 3. 29. 선고 2011도10508 판결
대법원 2014. 1. 16. 선고 2013도7101 판결

서울고등법원 2007. 8. 16. 선고 2007 노 929 판결
부산고등법원 2013. 6. 5. 선고 2012노667 판결
서울중앙지방법원 2007. 4. 16. 선고 2006고합1365 판결
서울중앙지방법원 2012. 11. 23. 선고 2011가합90267 판결

Comprehensive Drug Testing, 579 F. 3d 989,(9th Cir. 2009)
Riley v. California, 134 S.Ct. 2473 (2014. 6. 25.)
Hill, 459 F.3d 966, 974-75(9th Cir. 2006)
United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)
United States v. Evers, 669 F.3d 645(6th Cir. 2012)
United States v. Ganias, 755. F.3d 125(2nd Cir. 2014)
United States v. Joseph Schesso (9th Cir. 2013)
Westlaw, 2014 WL 7793690(2014. 12. 30.)

Abstract

A study on the relevance concept of digital evidence seized in the search : in the case of mobile forensics

Mu Young Lee
Department of Convergence Science & Technology
The Graduate School
Seoul National University

Digital evidence is characterized, which is mixed with other files that do not have necessarily the case with regard to the storage media massification. 2011 Criminal Procedure Code has been amended to that digital evidence is limited to those relating to search and seizure case. But that is in the field search and seizure techniques and temporal limits. The proviso in the Criminal Procedure Code that can be a source gave me a seizure the digital storage medium.

Investigators seized digital evidence that are easy to source the illusion that secured by a warrant that all data stored in the evidence. Investigators should try to use the issue to accept

evidence without a warrant, even if additional evidence is discovered for the additional crime in the digital evidence seized by a legitimate search warrant. If so, it is general warrants and unconstitutional. There are cases in relation to the above competence by excluding evidence illegally collected evidence on a cellphone recording files that are not related to the case of the Supreme Court. If the United States as well as the evidence relating to another case in which digital evidence is found to warrant further reported to be charged in court.

Electronic information must be included in the search and seizure in order to apply the subject of the case and the recent Supreme Court of the United States entering the country investigating reality. Court and law enforcement agencies will have to compensate for gaps in the law for the time being through seminars, conferences, etc.

Mobile phone(smartphone) is referred to as a gold mine of digital forensics. Has become much more important evidence has been discovered that infringe the privacy of individuals in proportion to that. Limited to those related to events in the cell phone confiscated and analyzed by the output and the copy must be careful not to infringe the individual's privacy. Mobile phone evidences have been stored sensitive personal information of individuals should be screened on a separate filtering team.

Finally, investigations and digital evidence to satisfy the efficiency of individual human rights on both sides of the investigation on the basis of this thesis is hope to be done.

Keywords : Digital Evidence, Digital Forensics, Mobile, Search · Seizure, Relevancy

student number : 2013-24054